Scout Enterprise Administrator's Guide

Date: 2015-04-24

Content:

0. Legal Information 1
1. Introduction 2
1.1. About Scout Enterprise Management Suite guide 2
1.2. Communication between thin client and Scout Enterprise Server 2
1.3. Representation 2
1.4. Shortcut keys 3
2. Installation 4
2.1. System requirements 4
2.2. System limitations 4
2.3. Support of databases 4
2.4. Installing Scout Enterprise 10
2.5. Installing Scout Enterprise unattended (silent installation) 10
2.6. Changing Scout Enterprise 11
2.7. Uninstalling Scout Enterprise 11
2.8. Encryption 11
3. Interface 12
3.1. Scout Enterprise interface 12
3.2. Symbols 12
3.3. Organization structure 13
4. Device management 14
4.1. General 14
4.2. Automatic device identification 14
4.3. Searching for devices (Discovery) 14
4.4. Executing the Reverse discovery 15
4.5. Reserving device profile 16

4.6. Secure device management with Scout Enterprise 17
4.7. Client relocation between servers 18
4.8. Dynamic client groups 22
4.9. OU filter 24
4.10. Printing device list 26
4.11. Searching for applications, devices or OUs 26
5. Setup 27
5.1. Introduction 27
5.2. General 30
5.3. Network 31
5.4. Screen 36
5.5. Security 38
5.6. Firmware 41
5.7. Multimedia 47
5.8. Desktop 48
5.9. Drives 50
5.10. Printer 52
5.11. Mouse/keyboard 59
5.12. Hardware 61
5.13. Diagnosis 62
5.14. VPN 63
6. Advanced settings 64
6.1. Devices 65
6.2. Update 65
6.3. Wake On Lan 66
6.4. Files 67
6.5. Advanced file entries 69
6.6. Rules 70
7. Defining applications 71
7.1. General 71
7.2. ICA 77
7.3. StoreFront 82
7.4. RDP 85
7.5. Browser 89
7.6. Local 91
7.7. PN-Agent 92
7.8. Emulation 95
7.9. SAP GUI 99
8. Online commands 100
8.1. Scheduling and executing commands 100
8.2. Mirroring 101
8.3. Executing the setup comparison 104
8.4. Device diagnostics 105
8.5. Setup of OUs/Comparing devices 107
8.6. Scout Enterprise commands for WES7 107
8.7. Switching OU to the highest level 107

9. Firmware Update 108
9.1. Requirements 108
9.2. Planning and performing an update via the network 109
9.3. Update Log 110
9.4. Update through proxy client 112
9.5. Troubleshooting 113
10. Passwords 114
10.1. Local device password 114
10.2. Changing Scout Enterprise console password 115
11. Managing administrators 116
11.1. Activating administrator management 116
11.2. Adding an administrator 116
11.3. Deleting an administrator 116
11.4. Administrator policy 117
11.5. Passthrough Authentication 121
11.6. Logging options 121
12. Statistic Server 123
12.1. About statistic server 123
12.2. Requirements 123
12.3. Defining status messages (keep alive message) 123
12.4. Examples of the status message 124
13. Communication of the console 125
13.1. Closing the console 125
13.2. Sending messages 125
13.3. Managing consoles 125
13.4. Managing commands 126
14. Import/Export 127
14.1. General 127
14.2. Exporting 127
14.3. Importing 127
15. Optimizing and troubleshooting 128
15.1. Optimizing with handshake 128
15.2. Error messages during Scout Enterprise setup 129
16. Appendix 130
16.1. Port assignments 130
16.2. SNMP 134
16.3. SNMPD and SNMP Configuration Directives 135

0. Legal Information

© 2015 Unicon Software GmbH.

The information provided in this document is protected by copyright. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, without the express consent of Unicon Software GmbH. Information in this document is subject to change without notice. Unicon Software GmbH disclaims all liability regarding correctness, completeness and topicality of the information contained herein and regarding any errors or damage resulting from the information provided.

eLux® is a registered trademark of Unicon Software GmbH in the European Community and the United States. eLux™ is a registered trademark of Unicon Software GmbH in Japan.
Scout Enterprise Management Suite® is a registered trademark of Unicon Software GmbH in the European Community. Scout Enterprise Management Suite™ is a registered trademark of Unicon Software GmbH in the US and in Japan.

All other trade names we refer to are service marks or trade marks of the respective manufacturers.

Unicon Software GmbH
Philipp-Reis-Straße 1
76137 Karlsruhe
+49 (0) 721 96451-0

1. Introduction

1.1. About Scout Enterprise Management Suite guide

Scout Enterprise Management Suite is the management solution for thin clients or PCs working with the operating system eLux®. Even the operating systems Windows Embedded, WinCE and Windows Embedded Standard 7 can be managed with Scout Enterprise to a certain extent.

Scout Enterprise supports the following operation systems:

- eLux® RL, eLux® RT and eLux® RP
- Windows CE® 5.0, 6.0
- WindowsXP Embedded
- Windows Embedded Standard 7

1.2. Communication between thin client and Scout Enterprise Server

During startup the client device connects to its Scout Enterprise Server asking for the latest configuration data.

There are three options:

- Client reaches the Scout Enterprise Server. The Scout Enterprise Server has no updated configuration data. Client continues booting with its configuration.
- Client reaches the Scout Enterprise Server. Scout Enterprise Server reports new configuration data and transfers the data to the thin client. If required, the client will restart using the new configuration.
- Client does not reach Scout Enterprise Server due to network or other problems which result in a management timeout (see Advanced network settings). The thin client continues booting with its configuration.

Updated configuration data can relate to device configuration (setup), application definition, files configured for tranfer and advanced file entries.

During operation of a client device there is no data exchange between Scout Enterprise Server and thin client. During shutdown, the client reports its current status to Scout Enterprise Server.

Exception: VPN Connections.

1.3. Representation

The following representations and conventions for instructions are used throughout the documentation:

Representation	Description
Control element	All graphical user interface controls are displayed **bold**
Menu > menu command	Whenever running a command involves clicking a series of menus , the single GUI controls such as menu commands or dialog tabs are linked by **>**.
`Value`	All data that have to be put in or that represent a field value are displayed in `Courier New`. Also, file names and path names are shown in `Courier New`.
STRG	Keys to be pressed are displayed in CAPITAL LETTERS.
Placeholder	Placeholders in syntax and in user input are displayed *italic*.

Representation	Description
1. Instruction	Procedures to be carried out step by step are realized as numbered steps.
Result	System's responses and results are displayed in *italic*.

Conventions

A group or organizational unit within the organization structure is called **OU**.

1.4. Shortcut keys

Shortcut	Selected icon	Description
CTRL-SHIFT-INSERT	Organization unit	Opens the dialog **Properties of Organisation unit**
	Applications	Opens the dialog **Application Properties**
	Devices	Opens the dialog **Information** to enter a MAC address
CTRL-SHIFT-DELETE	Organization unit	Deletes the selected organization unit
	Application	Deletes the selected individual application
	Devices	Deletes the selected individual device
F2	Organization unit	Renames the organization unit
	Individual device	Renames the individual device
	Individual application	Renames the individual application
F5		Updates the configuration of all devices
CTRL-F		Finds text in the tree view
CTRL + SHIFT + F		Opens the window Search.
CTRL-X	Individual device	Cuts the device
CTRL-V	Individual device	Pastes a device
CTRL-A	Applications devices	If focus is in the Properties window, select all applications / devices
CTRL-E	Individual device	Executes a **setup comparison**
CTRL- P		Opens the **print dialog** for printing the list of available devices

2. Installation

2.1. System requirements

Minimum system requirements for installing the Scout Enterprise Server:

- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows Vista, Windows 7, Windows 8
- Suitable ODBC driver
- In order to install the 64-bit version of Scout Enterprise (Scout Enterprise 14.0.0 or higher), the Microsoft® SQL Server® Native Clients or a suitable 64-bit ODBC driver for the Jet-Engine (AccessDatabaseEngine X64 Package) has to be installed on the Scout Enterprise Server. The corresponding MSI file (file name: ***sqlncli.msi***) can be downloaded on the Microsoft® web site separately or as part of Microsoft® SQL Server® Feature Pack. After successful installation of the Microsoft® SQL Server® Native Client, the driver is displayed in the ODBC data sources.
- Hard disk space 80 MB
- Database system MS SQL server or MS JETdatabase engine (mdb) which is included in Windows
- Administrator's rights for the system Scout Enterprise is running on.
- Administrator's rights for connecting to the TCP/IP network.

Minimum requirements for the container:

- Write access to FTP or HTTP server, local or via network.
- The required space depends on the container of the hardware installed and on the software available for this container. Also the memory capacity required depends on the installed software, which is currently available in this particular container. The minimum space required for all containers is: 700 MB (information at publishing time).

For more information, see www.myelux.com.

2.2. System limitations

There are no known system limitations concerning Scout Enterprise Management Suite and the Scout Enterprise console. Other services for example Citrix XenApp are able to run on the same system.

2.3. Support of databases

Scout Enterprise requires database software such as Microsoft JET database or Microsoft SQL Server.

The Microsoft Server operating systems already include Microsoft JET database. During installation of Scout Enterprise the Scout Enterprise Server can create a database of the type *.mdb with any name you wish.

Alternatively, you can use Microsoft SQL server 2000 or higher. In this case you have to install the database before installing Scout Enterprise.

We recommend Microsoft SQL server 2000 or higher.

The Scout Enterprise database requires about 50 MB free disk space per 1,000 devices.

Using the database connection editor you can define various database connections for the Scout Enterprise console. You then can select one or more of the defined connections when starting the console. From your console you can use multiple connections to different databases at the same time.

The database connection editor is provided in the start menu.

Note
If you already use Microsoft JET Database (.mdb) you can convert to SQL database while keeping all database information about configuration, devices and licenses. Contact support@unicon-software.com to coordinate the proceeding.

2.3.1. Authentication of the SQL server

If in the Setup menu SQL is used as a database type, you can choose from different authentication methods: SQL server authentication respectively Windows authentication.

SQL server authentication means: User name and password have to refer to a SQL server user.

Windows authentication – also called "trusted-connection" means: A program always logs on to the current credentials SQL server. No user or password are entered for the log on to the SQLserver. However, in this case the Scout Enterprise service must be run within a specific user account. Otherwise the service would run under the local system account which usually does not have the authorization in the SQL server. The user name and password of the service account may also be entered in the dialog.

Additionally there are two **Browse** buttons which shows a list of the available SQL servers respectively the available databases for you to choose from.

2.3.2. Defining application roles in the SQL server

In order to control access from the console to SQL server tables, it is possible to define an Microsoft SQL application role.The name of the application role must bedefined in the **System** table in the Scout Enterprise database.

1. Add a line with the ParamName='RName2' and ParamVal='<name of the role>' .
2. Add a line with ParamName='RPass2' and ParamVal='<password of the role>' .

During start of the Scout Enterprise console these fields are read and the applications role is set.

2.3.3. Scout Enterprise server cluster

If you use a SQL database, several Scout Enterprise servers can connect to the Scout Enterprise database concurrently. Concurrent Scout Enterprise servers enable failure load balancing as well as the possibility to configure load balancing using DNS entries (ManagerLoadBalancing).

Client devices that connect to Scout Enterprise server receive a list of all currently running servers that access the shared Scout Enterprise database.

FailureLoadBalancing

At start-up, the client tries to connect to the Scout Enterprise server it was connected to last time. If, however, that server is not available, it connects to the next server from the servers list. Subsequently, this one becomes the server the client tries to connect to by default.

The FailureLoadBalancing mechanism restarts as soon as the client fails to connect to the same Scout Enterprise server.

ManagerLoadBalancing

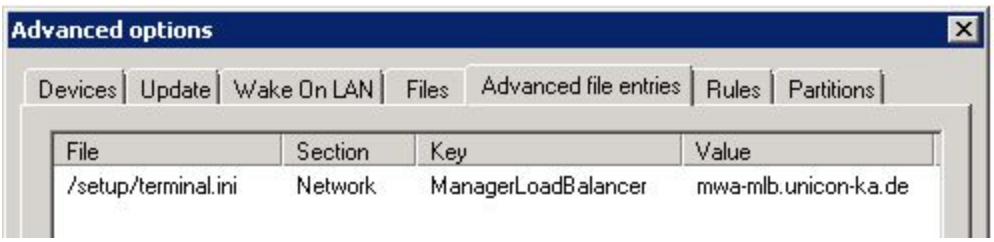
By setting the additional parameter

`ManagerLoadBalancer=`

in the `/setup/terminal.ini` file you can predefine a preferred server the clients are supposed to connect to.

This parameter can be set for all devices, for a OU or a single device. It is defined using the Scout Enterprise console feature **Advanced file entries**.

File	`/setup/terminal.ini`
Section	`Network`
Entry	`ManagerLoadBalancer`
Value	*<FQDN DNS entry>*



`ManagerLoadBalancer` refers to a DNS entry pointing to the relevant Scout Enterprise server. In a separate step the DNS entry must be defined on the DNS server. The DNS entry allows the assignment of devices to a particular Scout Enterprise server without modifying the device configuration.

The parameters `ManagerLoadBalancer` is interpreted by the devices on each client restart.

Outline process:

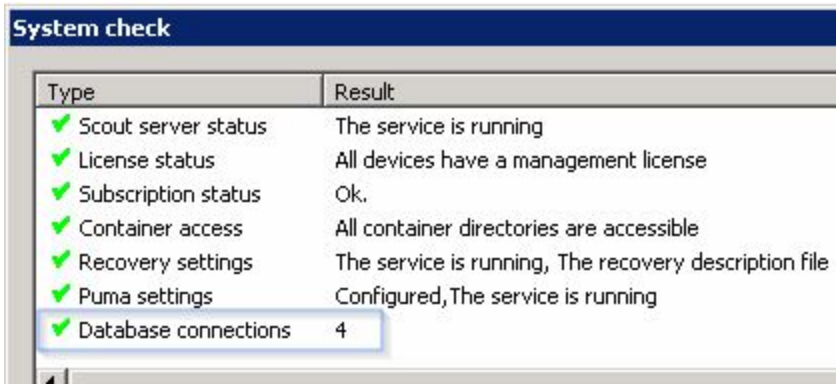
- Thin Client restarts
- DNS entry `ManagerLoadBalancer` is resolved
- Client connects to the determined Scout Enterprise server

If, however, the Scout Enterprise server identified by the DNS entry `ManagerLoadBalancer` is not available, the FailureLoadBalancing mechanism described above is used and the client connects to the next server from the list.

2.3.4. Number of ODBC connections

The number of ODBC connections between Scout Enterprise server and Scout Enterprise SQL database is defined dynamically at start-up of the server service. Normally, for each CPU kernel two ODBC connections are defined and used.

The number of database connections currently used can be viewed using the **system check** feature (Scout Enterprise console **View > System diagnostics > System check**).



From experience, two ODBC connections for each CPU kernel lead to good results considering

- maximum communication performance between Scout Enterprise server and SQL database and
- optimum CPU utilization.

Static versus dynamic ODBC connections

You can specify a fixed number of ODBC connections, to meet the particular system requirements of a Scout Enterprise installation. For this, you must define the following parameter in the configuration file `eluxd.ini` of Scout Enterprise server:

File	`%systemdrive%\Users\Public\Documents\UniCon\Scout\Server\eluxd.ini`
Section	`[ELUXD]`
Parameter	`DatabaseConnections=`
Value	`n` *(n=1-128)*

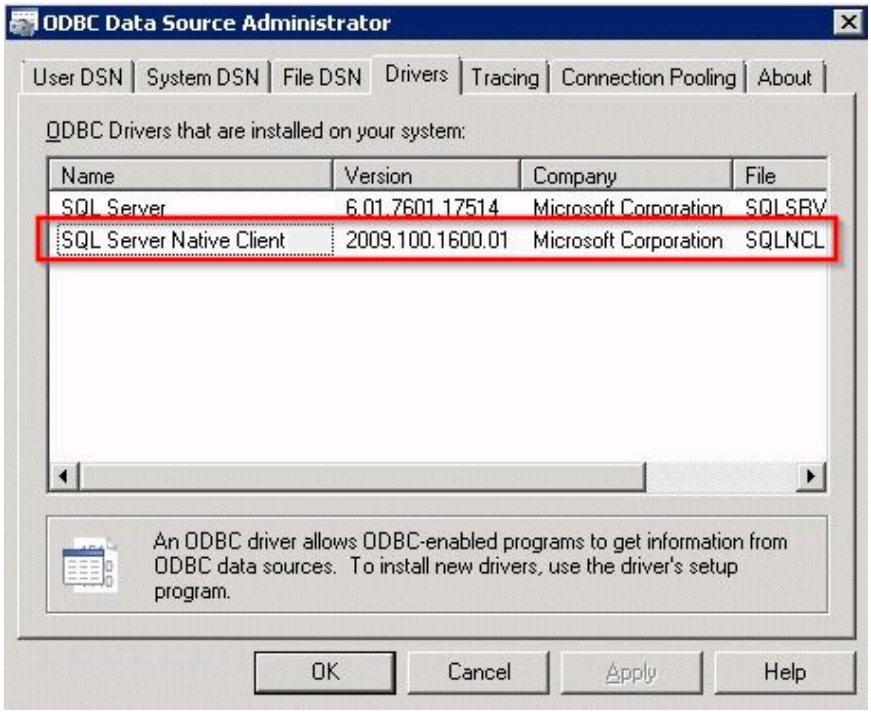
Note
Increasing the number of database connections manually can lead to CPU overload.

For more information on modifying `INI` files, see Advanced file entries.

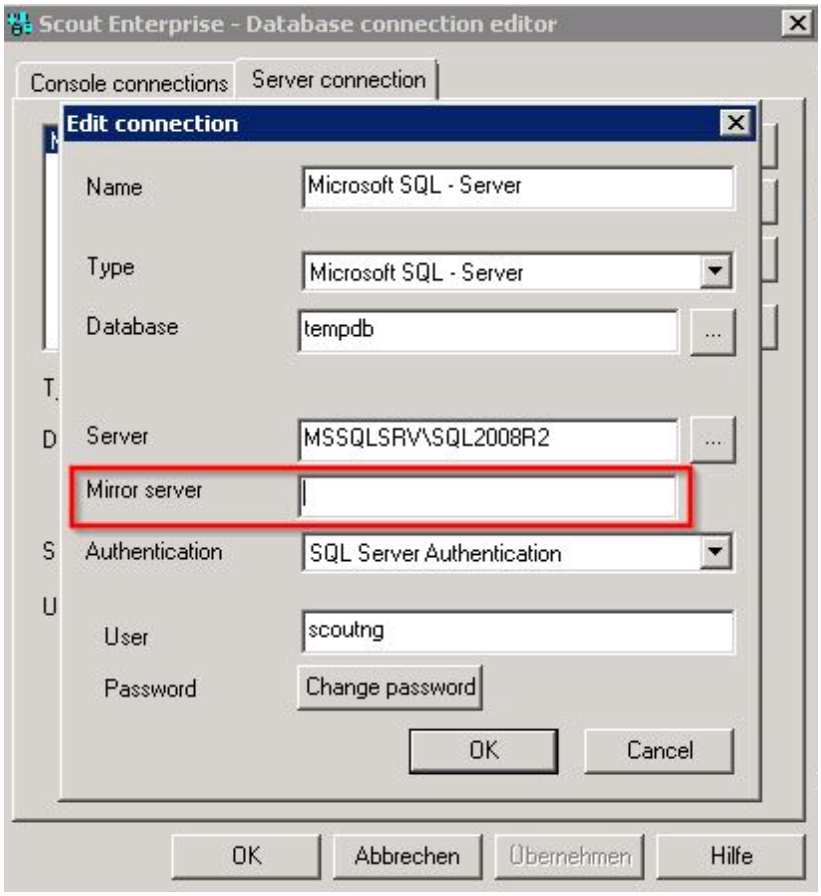
2.3.1. SQL server database mirroring

Starting from Scout Enterprise version 14.0.0, which can be downloaded on www.myelux.com, the Failover mechanism of the Microsoft® SQL Server® database mirroring is supported. In order to activate the support of the SQL database mirroring the installation of the Microsoft® SQL Server® Native Clients on the Scout Enterprise Server is necessary. The corresponding MSI file, (file name: ***sqlncli.msi***), can be downloaded as part of a Microsoft® SQL Server® Feature Pack. Alternatively the file can be downloaded separately on the official Microsoft® website.

After successful installation of the Microsof®t SQL Server® Native Client the driver appears in the ODBC data sources:



Subsequently, the mirroring server can be configured in the Scout Enterprise Database connection editor:



Note

In the case that the Microsoft® SQL Server® Native Client is not installed on the Scout Enterprise Server, the array Mirror server in the dialogue of the Scout Enterprise Database connection editor won't be shown.

After successful configuration of the Scout Enterprise Server in order to use the mirroring server, all the relevant Scout Enterprise components are now able to support the Failover database mirroring mechanism of the Microsoft® SQL Server®. However, it is important to ensure, that the user credentials of the particular user who accesses the database must be identical, regarding all the affected SQL server instances. Likewise, the Security Identifier (SID) is also affected. More details about the Microsoft® SQL server® database mirroring can be read in the Microsoft® documentation.

2.4. Installing Scout Enterprise

1. Download the latest version of Scout Enterprise here from our technical portal www.myelux.com.

> **Note**
> Execute the Setup from a local harddrive. Do not use a USB flash drive, CD-R drive or a network drive.

2. Run the file **Setup.exe** as administrator.
3. Choose the language option desired for executing the installation process.
4. Choose the desired type of installation. If necessary further software needs to be installed.
5. Confirm with **Install**.
6. Read the license agreement and accept.
7. Choose the desired type of installation and the memory location.
8. Choose the desired type of the database.
   It depends on the type of database, perhaps further settings concerning the user name or the password have to be executed. For further database settings see Support of databases.
9. Enter the first Organization unit (OU).
10. Enter language and time zone.
11. The next step is to define the applications you like to use.For more information, see Defining applications.
12. Start the installation process.

Scout Enterprise will be installed.

2.5. Installing Scout Enterprise unattended (silent installation)

You can install Scout Enterprise unattended (silent installation).
Activate the Scout Enterprise **Setup program** considering the following parameters:

```
setup.exe /s/v"/qn"
```

Option	Description
/v"UCPROP_DBTYPE=2"	0=Jet Engine, 2= MS SQL-Server
/v"UCPROP_DBNAME=Scout"	Demonstrates the name of the database
/v"UCPROP_DBSERVER=your-server"	Demonstrates the name of the server
/v"UCPROP_DBUSER=Scout-Admin"	Demonstrates the name of the administrator
/v"UCPROP_DBPASSWORD_ CRYPTED=u[D``Gqu[w_"	See also eluxd.ini
/v"UCPROP_OUNAME=your-OU"	OU in process
/v"UCPROP_DESKTOP_LANGUAGE-E=de_DE"	Demonstrates the desktop language settings

Option	Description
/v"UCPROP_KEYBOARD_ LANGUAGE=de"	Demonstrates the keyboard language settings
/v"ADDLOCAL=Feature1, Feature2 example: /v"ADDLOCAL=Console,Server,Report"	Installation of specific components. Make sure to enter this commands additionally and Individually by using the corresponding command.

Alternatively,you can extract the information manually from the file `eluxd.ini`, if you select controlled installation .The file `eluxd.ini` is located in the Scout Enterprise Server directory.

Possible features to execute a 64 bit installation:
Server
Console
Recovery
ELIAS
Report
Puma

Possible features to execute a 32 bit installation:
Server32
Console32
Recovery32
ELIAS32
Report32
Puma32

Of course the opportunity is given, to execute an unattended uninstalling by using the following command:
`setup.exe /x /s /v"/qn"`

2.6. Changing Scout Enterprise

1. Open the file Setup.exe.
2. Execute the installation program as usual.
3. Choose **Changing program**.
4. Choose from the program parts you like to install or uninstall and finish the installation process.

2.7. Uninstalling Scout Enterprise

Use the control panel to uninstall Scout Enterprise.

2.8. Encryption

The encryption between Scout Enterprise Server and the eLux clients is based on the AES (Advanced Encryption Standard). The clients in use have to run with eLux RL or higher respectively with eLux RP. Should a firewall be installed, Port 22123 must be unlocked.

3. Interface

3.1. Scout Enterprise interface

The category **Applications** shows a list of all applications in an OU. Using Drag&Drop you can move devices and applications from one OU to the other. For the devices the settings of the superordinate OU are applied.

Note
Assignment of settings from superordinate to subordinate levels is controlled by **Device configuration > General > Use parent**.

You can copy applications from one OU to another by Drag&Drop and pressing CTRL. For every OU you can change **Properties** and **Advanced Settings**. You can also define applications for every single OU. If you add a new device to an OU (either via Discovery or via moving of a device) it gets the configuration of this OU automatically.

The navigation panel can be hidden to show devices in a list. For this choose **View > Devices**. The list view shows devices without symbols. You can sort them via clicking at the header.

Via **View > Windows**you can show or hide certain windows:

Data category	Description
Device/ application list	Shows devices and applications as a list.
Properties	Shows properties of the highlighted application, OU or device.
Asset	Shows hardware information of the device.
Independent setups	
Compare setups	Shows differences in the configuration of two devices or OUs

3.2. Symbols

Symbol	Description
	Organization Unit (OU)
	Applications
	Device
	Device is turned on.
	Device is switched off or not available.
	Desktop is initialized. Log on screen is shown.
	Update is running.
	Not enough licenses available to manage this device.

3.3. Organization structure

By default the left side of the Scout Enterprise main window shows the complete organization structure with all devices in a tree view. At first log on you only see default applications and the default OU “Lost&Found".

To every OU you can add applications, devices and other OUs.

4. Device management

4.1. General

For managing a thin client architecture the MAC addresses of all clients must be known to the Scout Enterprise console. For this purpose different procedures are used. In this chapter you find useful information for managing thin clients equipped with eLux or Windows Embedded Standard.

4.2. Automatic device identification

During first boot procedure the thin client looks automatically for an available Scout Enterprise Server. In order that the particular Scout Enterprise Server will be identified, you have to modify either the DNS server or the Host name "ScoutSrv" or the DHCP option 222 according to the IP address of the particular Scout Enterprise Server.

Requirements:

- The configuration of the particular thin client must be in initial state.
- The particular thin client must be connected with the network.
- On the DNS server the host name "ScoutSrv" (no case sensitivity) must be assigned to the IP address of your Scout Enterprise Server.
- Alternative to using DNS the Boot/DHCP server can be used to predefine Scout Enterprise Server and OU for a particular thin client.

Execution:

- Turn the thin client on.

The configuration of the standard group will be assigned to the particular thin client. After a reboot the thin client is able to process the new settings.

4.3. Searching for devices (Discovery)

Requirements:

- The devices are turned on.
- The devices are equipped with valid IP addresses.
- The device password is known.

1. Choose **Options > search devices**.
2. Enter the following data:

Start address	First IP address in this particular section.
Counter	Number of all IP addresses in this particular section.
End address	Last IP address in this particular section.
Password	Standard password: elux
Target group	Particular OU, to which the device should be assigned

3. Confirm with **OK**.

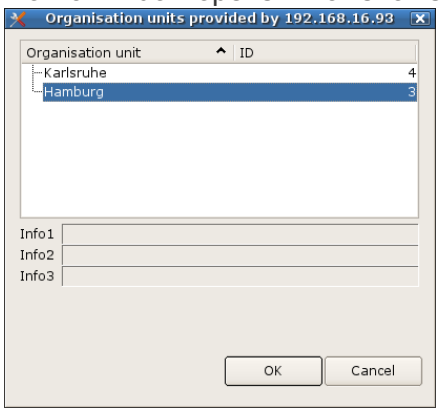
.

The devices will be assigned to the desired target group.

4.4. Executing the Reverse discovery

A reverse discovery is similar to a client discovery, except that management information entry takes place at the Thin Client

1. Choose in the eLux control panel **Setup > Security**.
2. Enter in the field Scout Enterprise the name or the IP address of the Scout Enterprise Server.
3. Click at**...**
   Now a window opens which shows all OUs available of this server.



4. Choose the desired OU.
5. Confirm with**Edit.**
   The devices has to be rebooted.
6. Confirm the window by clicking**OK**.
   Now the thin client reboots and will be directly assigned to the corresponding OU.

4.5. Reserving device profile

When manually creating devices in Scout Enterprise console the devices can be assigned to a particular OU even before they connect to Scout Enterprise server for the first time.

As soon as a manually created device contacts its Scout Enterprise server for initial start-up, the already defined MAC address is recognized and configuration data of the OU is transferred to the device.

This procedure can be applied for

- Discovery
- Reverse Discovery
- DNS alias name `ScoutSrv`
- DHCP option `222` for Scout Enterprise-server

Note
If there is a OU filter enabled, the OU filter precedes device profile reserving.

Reserving device profile

1. Select the relevant OU the device shall be assigned to, and show its subtree.
2. Open the context menu of **Devices** within the OU and select **Add...**
3. Enter the MAC address of the device.

   *If it is a valid MAC adress, the **Setup** dialog opens. The **Use parent** option is selected.*
4. Confirm with **OK**.

4.6. Secure device management with Scout Enterprise

Scout Enterprise V13.4.x and higher provides an enhancement to the connection security of new clients which are added in the Scout Enterprise console. Clients which have their MAC address saved in the Scout Enterprise database will be accepted by the Scout Enterprise Server and can be managed by Scout Enterprise. It is ensured, however, that clients with an unknown MAC-address will not be accepted by the Scout Enterprise database and for this reason they cannot be managed by Scout Enterprise. Unaccepted clients will not be assigned any license from Scout Enterprise's license pool. Thus, an additional security level is guaranteed.

Setting up Scout Enterprise

- Start Scout Enterprise **> Options > Advanced options > Devices > New**.
- Activate the checkbox **Accept only known devices**.

If an unknown device tries to contact the Scout Enterprise Server, an error message is displayed on the client saying that there is no connection possible to the Scout Enterprise Server.

4.7. Client relocation between servers

Relocating devices from one Scout Enterprise server to another can be very helpful in different scenarios relating to device migration. For example, devices are supposed to be relocated from test/QA server to production server or several Scout Enterprise servers are to be consolidated to a single server (server fusion).

Requirements: Scout Enterprise V14.3.0 or later, eLux RP V4.8.0 or later

4.7.1. Relocation procedure

The relocation procedure is initiated by the source server (device-releasing server) and completed by the target server (device-receiving server). The actual relocation procedure, however, is performed by the client and includes the required testing of the surrounding conditions, the transfer of client licenses and the proportional subscription validity.

Relocation is triggered by the notification **Initiate client relocation** for the relevant devices in Scout Enterprise console of the source server. On the next client reboot, the configuration data of the target server is replicated and the clients evaluate the relocation notification.

The clients then check the target server's address that has been transmitted on availability via network. Moreover, the clients verify the Scout Enterprise version of the target server (V14.3.0 or later). Relocation is only executed by the clients if the test result is positive.
Along with the target server address, the clients are provided with information on their licenses and proportional Subscription validity by the source server. This information is to be transmitted to the target server.

After having successfully checked availability of the target server and valid Scout Enterprise version, the devices are deleted from the source server along with their licenses and subscription.

The clients establish a connection to the target server and transmit the license and subscription information they have received from the source server. The target server's amount of licenses and subscription is updated accordingly.

The new clients on the target server are assigned to the OU configured as default (see Scout Enterprise console: **Options > Advanced options > Devices > New devices**). If you have enabled an OU filter, the devices are assigned automatically in accordance with the filter rules.

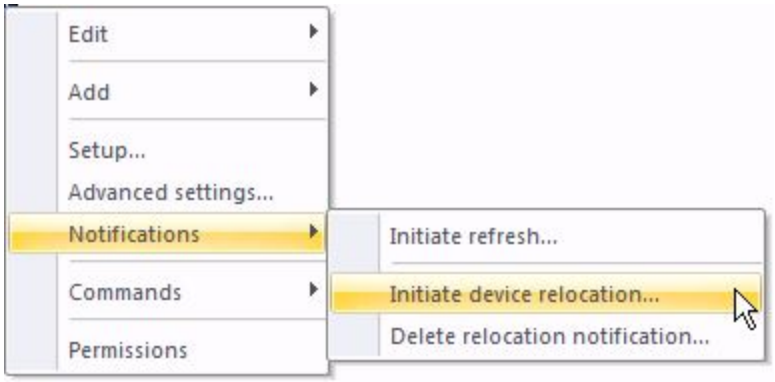
To complete the relocation procedure the clients must be restarted to activate the configuration of the target server. If the OU filter is used, an additional restart of the clients is provoked by the system right after assignment.

Important

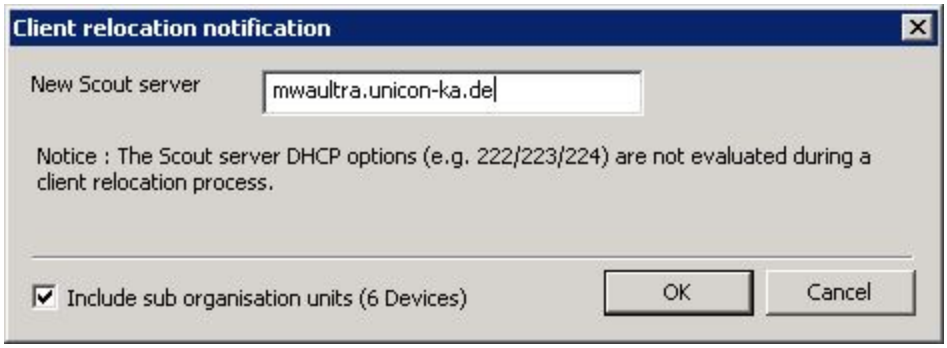
Do NOT reserve device profiles by entering the MAC addresses of the new devices on the target server before client relocation. If the devices are already registered on the target server, licenses and subscription will NOT be updated. Before client relocation, in **Advanced Options > Devices**, clear the **Accept only known devices** option on the target server, if selected.

4.7.1. Initiating client relocation

1. For the relevant OU, device or dynamic device group, open the context menu and select **Notifications > Initiate client relocation...**.



2. In the **Client relocation notification** dialog, enter the name (FQDN) or the IP address of the target server.

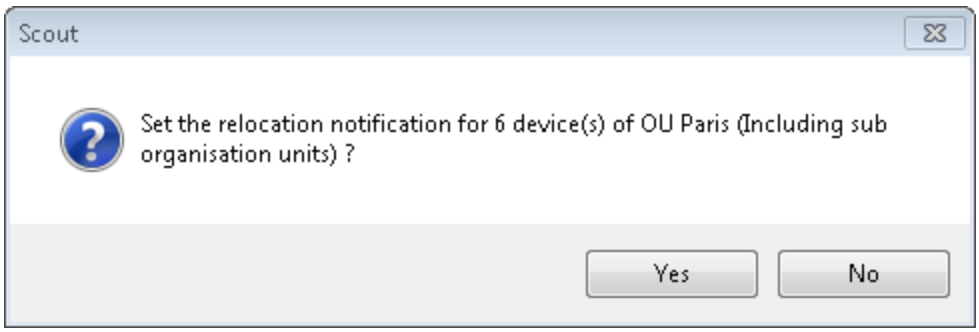

Client relocation notification
New Scout server
mwaultra.unicon-ka.de
Notice : The Scout server DHCP options (e.g. 222/223/224) are not evaluated during a client relocation process.
Include sub organisation units (6 Devices)
OK
Cancel

If you want to include the devices of all subordinate OUs, select the option **Include sub organisation units**. The number of devices shown in brackets will be updated dynamically.

Note
The DHCP options of the client are not checked during relocation to ensure relocation success in any case. If, however, DHCP options for the source server have been defined, you must select the **Ignore DHCP options** option in the device setup **Network > LAN > Edit > Advanced** on the target server.

The name of the target server is resolved, or the IP address is verified, respectively.

3. Confirm the following message after having checked the number of devices to be relocated.



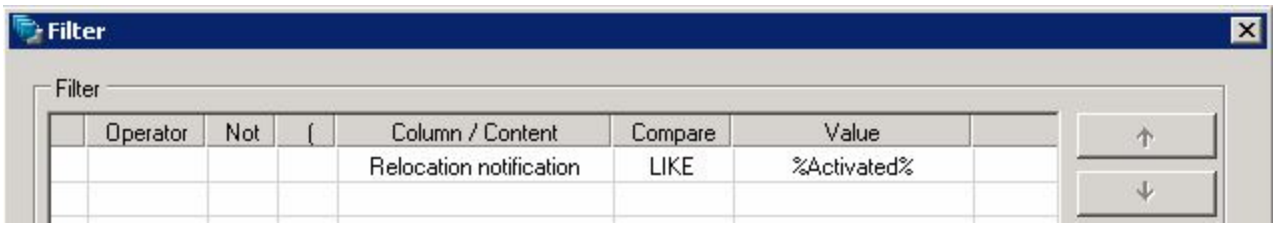
*The notifications for client relocation are set. For each device the current status of the **Relocation notification** is shown in the **Properties** window.*

Relocation notification	Activated (mwaultra.unicon-ka.de / 192.168.16.57)

*If a device is not concerned by relocation, the **Relocation notification** field remains empty.*

Note
Possibly, you must show the field **Relocation notification** in the **Properties** window by using .

Using Scout Enterprise Report Generator, you can analyze those devices having an activated relocation notification:

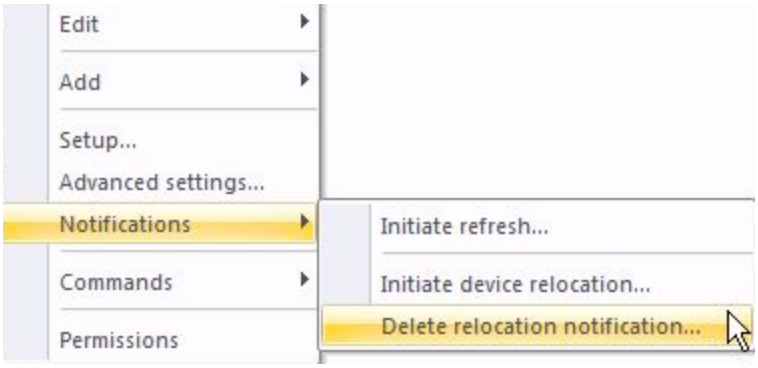


4. If you want to control execution of the client relocation, use Report Generator to identify and export the relevant devices to a dynamic device group, and then run the command **Restart device...** on that group.

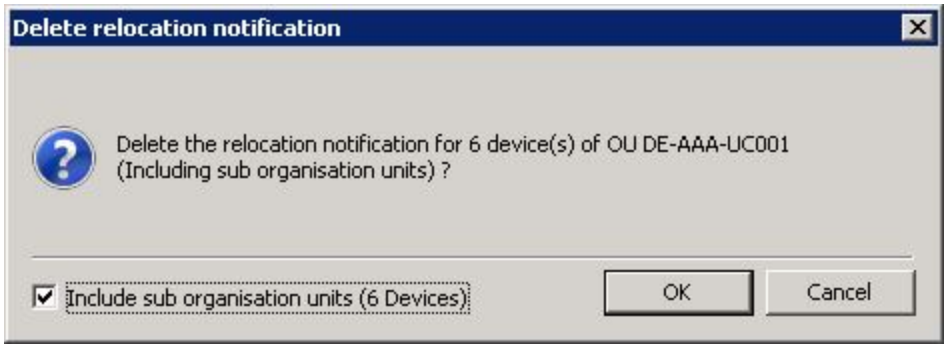
   The relevant devices are restarted at the point in time defined by you and get their configuration data from the target server. That way you can ensure that relocation takes place beyond working hours and that all relevant devices are relocated at the same time.

4.7.1. Deleting relocation notification

1. For the relevant OU, device or dynamic device group, open the context menu and select **Notifications > Delete relocation notification...**.



2. If you want to include the devices of all subordinate OUs, in the **Delete relocation notification** message, select the option **Include sub organisation units**.


Delete relocation notification
Delete the relocation notification for 6 device(s) of OU DE-AAA-UC001
(Including sub organisation units) ?
Include sub organisation units (6 Devices)
OK
Cancel

The number of devices shown in brackets are updated dynamically.

3. Confirm with **OK**.

*After refreshing the **Properties** window, the **Relocation notification** status for the relevant devices has been deleted.*

4.8. Dynamic client groups

Dynamic device groups enable administrators to run cross-OU commands for freely definable device groups. For example, you can send a message to all devices with a particular image throughout the whole organization. Or, you can run a BIOS update on all devices with a particular BIOS version, across all OUs. Even client relocation to another Scout Enterprise server can be applied to a dynamic client group.

Dynamic client groups are based on reports created in Scout Enterprise Report generator which extract the desired devices. These reports are exported once to Scout Enterprise console, and from that point onward, are displayed as **Dynamic client group**. Any commands applicable to OUs or to single devices can be applied to a dynamic device group.

Dynamic client groups are displayed in Scout Enterprise console in a special window and remain there for re-use until they are deleted. They can be updated any-time by one click.

When creating dynamic client groups, access rights are respected as defined in administrator management.

4.8.1. Requirements for dynamic client groups

- Scout Enterprise Management Suite 13.4.2 or later
  Download on www.myelux.com.
- Scout Enterprise Report generator of Scout Enterprise Version 13.4.2 or later
- Report layout must include the MAC address

For more information on defining dynamic client groups, see Creating dynamic client groups in Scout Enterprise Report generator manual.

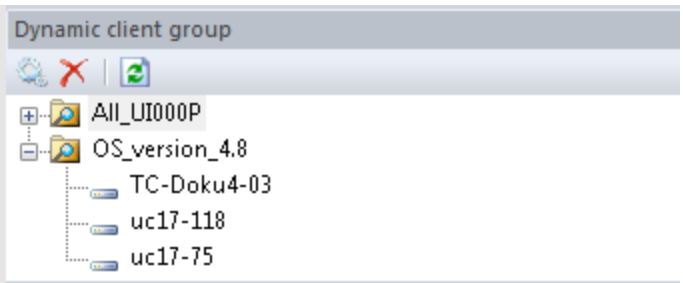
4.8.2. Using dynamic client groups

Dynamic client groups are based on reports that have been created in Scout Enterprise Report generator and exported to Scout Enterprise console.

For more information on defining and exporting, see Creating dynamic client groups in Scout Enterprise Report generator manual.

Displaying dynamic client groups

- In Scout Enterprise console, click **View > Window > Dynamic client groups...**.



*The **Dynamic client groups** window is displayed. The dynamic client groups can be expanded to show the matching devices.*

Note
The dynamic client group shows those devices that have matched the criteria at the time of the latest report generation. Make sure that the dynamic client group is up-to-date.

For a selected dynamic client group, the **Properties** window shows **Creation date**, **Number of devices** and **Filter** of the used report. The creation date refers to the date of the latest generation of the report the dynamic client group is based on, and thus indicates if the dynamic client group is up-to-date.

If, for example, new devices have been integrated into the database and these devices match the criteria of the report, the dynamic client group is not up-to-date any longer. You can, however, update the dynamic client group by re-creating the report right from Scout Enterprise console.

If a dynamic client group is not needed anymore, you can delete it by using the ✕ button. The report the dynamic client group was based on remains unaffected.

Updating dynamic client groups

1. In the **Dynamic client groups** window, select the relevant client group.
2. On the toolbar of the **Dynamic client groups** window, click the **Re-create** button .

*The relevant report is re-created and exported. The resulting devices are shown below of the dynamic client group as extracted from the database. In the **Properties** window, in the **Creation date** field, the current point of time is displayed.*

Note
The **Refresh** button refers to the view only. The report is not updated by this command.

Applying commands to dynamic client groups

1. In the **Dynamic client groups** window, select the relevant dynamic client group.

   *In the **Properies** window, the values of the fields **Creation date**, **Number of devices** and **Filter** are displayed.*

2. Update the dynamic client group using the **Re-create** button to make sure that all currently matching devices are concerned.
3. Open the context menu of the dynamic client group and select the desired command.

Commands and notifications are applied to the matching devices, irrespective of their OU. The available commands can also be scheduled for later execution.

4.9. OU filter

4.9.1. General

The OU filter can be used for automatic assignment of devices to an organization unit (OU) based on defined criteria. The OU filter can use either the client network adress (**Subnet filter**) or any configured asset information of the devices (**User-defined filter**) for filtering.

The OU filter has **higher priority** than

- OU mapping of devices via DHCP option 223
- search for new devices via Scout Enterprise
- local OU selection in the First Configuration Wizard on the thin client.

4.9.2. Setting up an OU filter as subnet filter

You can use the OU filter to filter on client network addresses.

1. Click **Options > Advanced options... > Devices**.
2. Check the option **Assign OU depending on the OU filter** , and then click **....**
3. In the **Filter type** list, click `Subnet filter (client network address).`
4. In the **Network address** box, enter the scope of IP addresses.
   For example 192.168.16.0 covers all IPs starting with 192.168.16.
5. In the **OU** list, select the OU the devices shall be assigned to. Click **...** to browse.
6. Click **Add**.
   The filter criterion will be displayed in the list below.
7. In the list **Non-matching devices will be** click one of the options.
   Decide where you want the devices to go that are not matching the filter criterion.
   Note: If you select `assigned to the default OU`, all non-matching devices and even devices that are already assigned to other OUs will be reassigned to the default OU.
8. Click **OK**.

On the next reboot the devices will be assigned to the OUs as defined by the OU subnet filter.

4.9.3. Setting up an OU filter as user-defined filter

You can filter on configured asset informations of the devices. Devices with eLux RP V.4.6.0 and higher send a **OU filter text** field containing device information about themselves to the Scout Enterprise Server. You can use the field **OU filter text** in the report generator and for the user-defined OU filter. It includes the values for the following features: host name, OS name, OS version, serial number, supplier, device type, BIOS, CPU speed, model,kernel version, flash type, flash size, RAM size, graphics.

1. Click **Options > Advanced options... > Devices**.
2. Check the option **Assign OU depending on the OU filter** , and then click **....**
3. In the **Filter type** list, click `User-defined filter (configured asset information)`
4. In the **Filter rule** box, enter one or several strings from the **OU filter text** you want to be used as filter criterion.
   You can combine several strings using AND and/or OR.
   Example for the values of an **OU filter text** field:
   ELUX_HOSTNAME=Inga;ELUX_OSNAME=eLux RP;ELUX_OSVERSION=4.6.0-1; ELUX_SERIAL=44015379;ELUX_SUPPLIER=FUJITSU;ELUX_DEVICETYPE=D3314-A1; ELUX_BIOS=V4.6.5.4 R1.4.0 for D3314-A1x;ELUX_CPU=998;ELUX_PRODUCT=D3314-A1; ELUX_KERNEL=3.4.71;ELUX_FLASH=4GB NANDrive;ELUX_FLASHSIZE=3849; ELUX_

MEMORY=2048;ELUX_GRAPHICS=ATI AMD Radeon HD8210E
Example filter criterion 1: ELUX_OSNAME=eLux RP AND ELUX_OSVERSION=4.6.0
Example filter criterion 2: ELUX_DEVICETYPE=D3314-A1 OR ELUX_DEVICETYPE=D3003-A1

5. In the **OU** list, select the OU the devices shall be assigned to. Click **...** to browse.
6. Click **Add**.
   The filter criterion will be displayed in the list below.
7. In the list **Non-matching devices will be** select where you want the devices to go that are not matching the filter criterion.
   Note: If you select `assigned to the default OU`, all non-matching devices and even devices that are already assigned to other OUs will be reassigned to the default OU.
8. Click **OK**.

On the next reboot the devices will be assigned to the OUs as defined by the user-defined OU filter.

4.9.4. Deactivating OU filters for individual devices

1. For the relevant device, open **Advanced settings > Management**.
2. Under **New devices**, check the **Ignore OU filter** option.
3. Click **OK.**

Or:

1. By using drag & drop relocate the device in another OU.
2. Click **OK**.

A message will confirm that the OU filter is deactivated.

4.9.5. Deleting OU filters

1. Click **Options > Advanced options… > Devices**.

*The **Advanced options** dialog opens.*

2. Under **New devices**, next to the **Assign OU depending onthe OU filter** option, click **...**
3. Select the filter you like to delete.
4. Click **Delete**.

4.10. Printing device list

1. Chose **File > Print**.
   The window print opens.
2. Choose a printer and page size and confirm with **OK**.

4.11. Searching for applications, devices or OUs

1. Select **Edit > Find...**.
2. Enter the name of the application, device or OU you want to search for.

   Or: Enter the search term directly into the field **Search**

in the tool bar.

5. Setup

5.1. Introduction

Talking about how to efficiently manage a large number of thin clients, device configuration is a key feature. You will tend to configure as many clients as possible in the same way in order to keep IT processes simple and at low costs. All the same different locations, heterogeneous hardware environments and additional requirements do not allow unified configuration.

Scout Enterprise Management Suite reflects this situation by using inheritance: By default, the base configuration defined at top level will give its properties down to single device level.The concept of inheritance helps you keeping configuration consistent and efficient. To define any variations, just modify the relevant settings. Scout Enterprise provides flexibility to override any settings on all levels.

Note
Any changes to device configuration take effect on the next reboot of the relevant clients.

5.1.1. Inheritance of configuration

Base configuration and the configuration of OUs can be inherited to lower instances.

The base configuration is the top level instance. Lower instances can be other OUs or single devices.

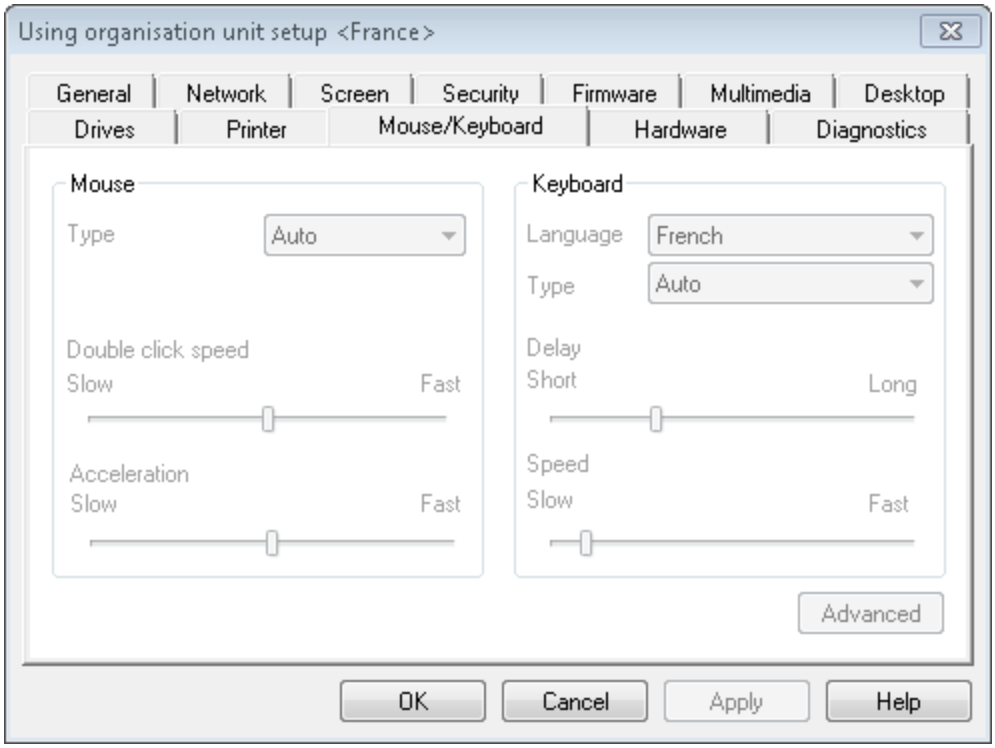
If the option **Use parent** is active, the configuration of the next level element of the hierarchy is applied to the current instance. By default, the option **Use parent** is active, so that a device inherits its configuration from the base configuration.

Settings of the configuration can be edited on three levels in Scout Enterprise console:

- Base configuration (**Options > Base configuration**)
- OU (**context menu > configuration**)
- Device (**context menu > configuration**)

On every level you can inherit the configuration from the superior level or define deviant settings. To be able to override settings, you must block inheritance, that is disable the use of parent configuration.

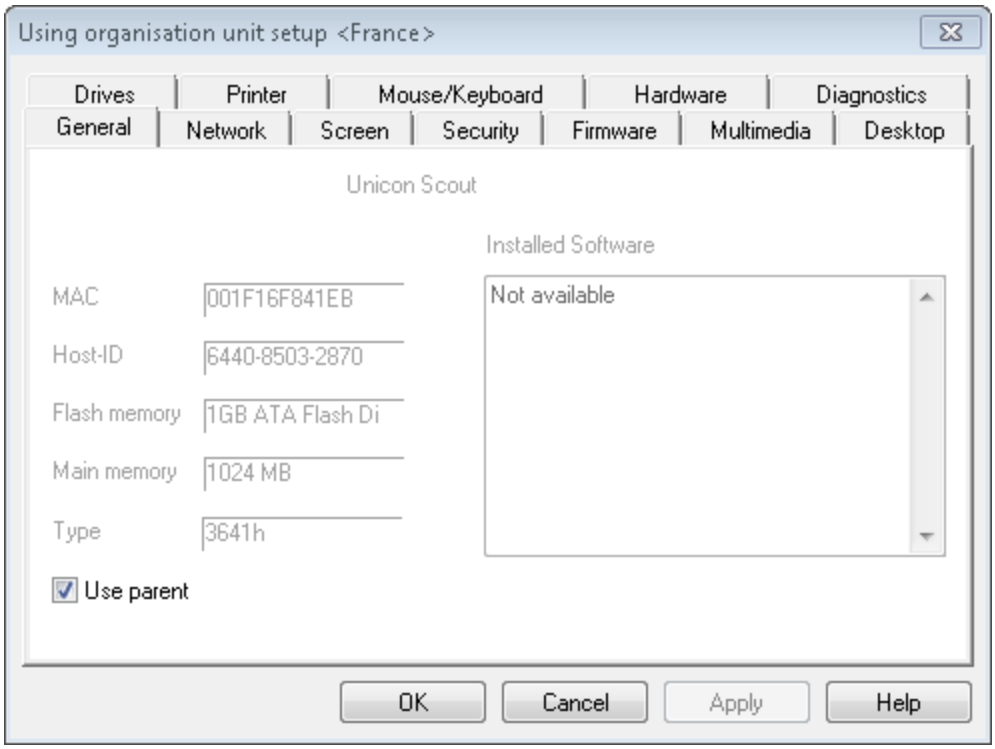
Note
Pay attention to the configuration dialog title. It indicates the location of the current configuration. This can be the base configuration or a superior OU.



Example: If inheritance is active and you open the configuration dialog of a device or OU subordinate to `France`, the title bar shows **Using organisation unit setup <France>**. To modify any settings you must open the `France` configuration dialog.

5.1.1. Blocking inheritance

If you want to define deviant settings for a prticular OU or device, you have to block inheritance for that instance.



1. Open the context menu of the relevant instance (OU or device) and click **Setup...**.

   *The **Setup** dialog opens and the title bar shows the currently active configuration instance. This can be the base configuration or a superior OU.*

2. Select the **General** tab.
3. Clear the **Use parent** option .

Inheritance is disabled. The title bar of the dialog shows the currently edited instance and the available options are editable. This instance and all subordinate instances can be configured independently of the superior instances.

5.2. General

In the **General** tab you can find information concerning the hardware. Since this information depends on the devices in use it is only shown in the configuration of a single device.

Date	Description
MAC address	The device addresses of the hardware (MAC=Media Access Control).
Host-ID	The eLux Host-ID is connected to the thin client. This is important regarding licensing process.
Flash memory	Short overview regarding flash memory type and the size.
Main memory	Main memory size in megabyte.
Type	Product details provided by the hardware manufacturer (character string).

Note
Also, the **General** tab contains the **Use parent** option. It may be useful to disable inheritance temporarily in particular situations. For more information, see Blocking inheritance.

5.3. Network

5.3.1. Connecting to LAN or WLAN

Depending on the image installed and the integrated hardware you can set up different network connections.

1. In Scout Enterprise for the relevant device or OU open **Setup > Network**. The same dialogue works for eLux on the client.
2. Select the desired connection tab.
3. Click the **Add** button.

   *The **Profile** dialog for Lan or WLAN opens.*
4. On the **IP** tab, determine whether the IP address will be dynamic or fill in all particular IP address data.
5. If you set up a WLAN connection, on the **Medium** tab fill in the fields **SSID**, **timeout**, **channel** and **method of encryption**.

Note
Due to security reasons the encryption methods: `None` or `WEP` are not supported any more. This affects especially the current operating systems eLux RP and eLux RT.

6. If you define a WLAN connection, check the **Connect automatically** option.

Note
If the **Connect automatically** is not checked, there is no automatic use of any WLAN connection.
In this case you have to activate the WLAN connection manually using the systray at the client.

7. On the **Advanced** tab you can choose further security options regarding DHCP or IEEE 802.
8. Click **OK** to save the settings of the **Profile** dialogue.

Note
If you wish to transfer the local host name of a particular device to the DHCP server, enter the host name in **Advanced Settings > Info** of the relevant device. On the Thin Client the field **Host name** is to be found in **Setup > Network**.

For advanced WLAN settings using the configuration file *wpa.conf* see Advanced WLAN Settings.

5.3.1. Advanced network settings

In **Setup > Network > Advanced** you will find the host list as well as features related to all network connections.

Defining a timeout for a connection:

- At **Management Timer** in the relevant fields enter the desired timeout time in seconds
  - when establishing a connection.
  - when the connection is in idle state.

After the indicated time, the connection will be canceled.

Defining a host list for networks without DNS server

If the network is not equipped with a domain name server (DNS), host names can be resolved locally by the device. All you need is to keep your host list up-to-date.

1. Click at **New**.
2. Enter the desired host name and the IP address.
3. Confirm with **OK**.

When rebooting, the host list will be transferred automatically

5.3.1. Advanced WLAN security settings

After having set up a WLAN connection (see Connecting to LAN or WAN) you can turn WPA encryption more secure by changing keys regularly. Using the `WPA-supplicant` software you can create the configuration file `wpa.conf` that will be imported into the database.

`WPA-supplicant` is a free software implementation. For more information about wpa_suppliant see http://w1.fi/wpa_supplicant/.

1. Create the configuration file *wpa.conf* with the help of the program: wpa_supplicant.

1. In Scout Enterprise console for the desired device or OU, click **Advanced settings... > Files**.
2. Click **Add**.

   *The dialog **Add file entry** opens.*
3. Check the **Import file to database** option.
4. Click **...**, and then select the configuration file *wpa.conf* from the file system.
5. In the **Destination file** box, set the path for the client to */setup/wlan/wpa.conf*.
6. Confirm with **OK**.

The settings will take effect on the client on the next boot.

Note
For more information about configuring a file list see Advanced configuration\Files.

5.3.1. Establishing a connection via 3G/UMTS

1. Choose **3G/UMTS > Add**.
2. Enter the following fields:

Option	Description
Name	Enter a name desired.
APN	Access Point Name. This is the system access point of the provider.
Timeout	Enter the timeout value desired in seconds. After those time period defined eLux is going to cancel the connection.
User name	The user name assigned by your provider.
Password	The password assigned by your provider.
PIN or SIM card	The PIN of your SIM card assigned by your provider.
Secured	This security option causes that local users are not able to modify the profile.
DNS server 1	If necessary enter a name server.
DNS server 2	If necessary enter a name server.

3. Confirm with **OK**.

5.3.2. Establishing a connection via ADSL

1. Choose **ADSL > Add**.
2. Enter the following fields:

Option	Description
Name	Enter a name desired.
Timeout	Enter the timeout value desired in seconds. After those time period defined eLux is going to cancel the ADSL connection.
User name	The user name assigned by your provider.
Password	The password assigned by your provider.
Identification	The protocol used by your provider.
Secured	This security option causes that local users are not able to modify the profile.

3. Confirm with**OK**.

When using ISDN, ADS or a modem eLux supports the dynamically change of IP addresses.

5.3.3. Establishing a connection via a modem

1. Click **Modem > Add** .
2. Enter the following fields:

Option	Description
Name	Enter the name you wish.
Telephone number	Enter the telephone number of your provider.
Timeout	Enter the time out period in seconds. After the defined standby time eLux is going to cancel the connection.
User name	The user name assigned by your provider.
password	The password assigned by your provider.
Identification	The protocol used by your provider.
Tempo	Choose the list of the desired baud rate for your modem. The setting has to be higher than the highest baud rate of the modem in use.
Secured	This security option ensures that local users are not able to modify the profile.

3. Confirm with **OK**.

When using ISDN, ADS or a modem eLux supports the dynamic change to IP addresses.

5.3.4. Establishing a connection via ISDN

1. Click **ISDN > Add**
2. Edit the following fields:

Option	Description
Name	Enter any name desired.
Telephone number	Telephone number of your provider.
Timeout	Enter the timeout value desired in seconds. After the time period defined eLux is going to cancel the connection
User name	The user name assigned by your provider.
Password	The password assigned by your provider.
MSN	Number for multiple ports. In the case you like to use a call back function enter your telephone number without dialing code. In the case you do not use a call back function enter 0 (zero).
Identification	The protocol used by your provider.
Recall	Activate the checkbox in the case your provider offers a call back function.
Using IP address	Activate the checkbox in the case your provider reserves a static IP address regarding your eLux terminal.
Secured	This security option prevents that local users are able to modify the profile.

3. Confirm with**OK**.

When using ISDN, ADSL or a modem eLux supports the dynamic change of IP addresses.

5.4. Screen

5.4.1. Customizing screen settings

On the **screen** tab you can define the basic settings concerning screen resolution, frequency as well as the color depth. Furthermore, you can define the use of multi monitors (dual monitors up to 4 monitors), energy saving options as well as screen saver with password.

Note
Higher screen resolution and high color depth require more graphics- and main memory capacity. It is therefore possible that the number of parallel opened applications is limited.

Defining multiple monitors:

1. In the **Number of monitors** list, selet how many monitors you like to connect to this thin client.

   As soon as more than one monitor is defined, all monitor icons are displayed on the left, and the additional sub tab **Order** *is displayed next to the* **Resolution** *tab.*

2. Select one of the monitor icons.
3. On the **Order** sub tab, determine its position in relation to the other monitors, as desired.
4. If you want this monitor to be the primary one, check the **Primary monitor** option.
5. On the **Resolution** sub tab, set screen resolution, frequency and rotation, as required.
6. If you want the values supported by the monitor to be processed by the client, check the **Use monitor Plug&Play Info (DDC)** option.
7. Select the next monitor icon and repeat the above steps to configure the monitor.

Important
If your monitors do not support the settings you have defined, you might have to set back the client to initial state and try to modify the desired screen settings again.

5.4.1. Setting screen saver

1. Define via the checkbox whether the screen saver should be activated or not.
2. Define via the field after how many minutes the screen saver should be activated.
3. Define via the checkbox if a user password is essential for unlocking the screen. In the case a authentication server is activated the password for using the screen saver is: $ELUXPASSWORD.
4. Click **Settings**, for choosing a screen saver and to configure this screen saver.
   A further window opens. The settings vary depending on which screen saver is activated.
5. Confirm with**OK**.

5.4.2. Configuring a font server

Using a font server you can easily manage different fonts. These fonts can be saved on server and can be requested on demand by a thin client.

1. On the **Screen** tab click **Advanced**.

2. In the **Advanced Screen Settings** dialogue click at **New**, **Edit** or **Delete** to define or modify or delete a font server. The following window opens:
3. In the **Define Font Server** dialogue in the **Font Server:Port** field enter IP address or IP name of the font server and then the port number. Use the following format: `<Fontserver IP-Adress>:<Port number>`, for example `192.168.10.23:7100`
   Or: In the **Font path** field and enter the path name where the fonts are installed.
   For example: `/smb/g/fonts`.

5.4.1. Turning on Backingstore

Backingstore saves the screen information locally on the X11 server of the thin client. The `pixmap` picture of every window is stored on the X server regardless of whether it is visible or not.

The general idea of this function is that during focusing a window, that means in the moment those window appears in the foreground again, the window picture must not be transferred again by the application but the X server fades the window in. Therefore, the screen view is faster constructed in the case the network connections works slowly.

This function makes sense when using slow network connections like ISDN. The single pixmaps are saved in the main memory, that means the X server needs more memory space. Backingstore requires at least 128 MB main memory capacity.

- Click **Screen > Advanced**.
- Check the **Backingstore** option.

5.5. Security

5.5.1. Configuring mirroring

Note
Mirroring can be disabled on the client.

1. On the **Security** tab, under **Mirroring**, check the **Enable** option.
2. Click **Advanced** for configuration:

Option	Description
Password	If desired, enter a password that will be prompted when starting a mirroring session.
Read access only	Allows read access only.
Confirmation needed	Before mirroring, the user has to confirm.
Transfer mirroring information	Enables recording of the mirroring session.
Encrypted transmission	Uses encrypted transmission.
Allow Scout Enterprise only	Mirroring is only allowed by Scout Enterprise Server.
XDMCP	Enables the XDMCP protocol

3. Confirm with **OK** and **Apply**.

For more information on starting a mirroring session, see Mirroring devices.

5.5.1. Local Security

Allowing remote connections to X11 clients

Due to the activation of X11 applications which are hosted on remote servers, these applications can be shown in eLux.

- Choose **Allow remote X11 clients**.

Changing user authorizations

1. In the **Security** tab, under **Local Security** click **Edit**.
2. Enter the device password.
3. Turn the features on or off using double click or SPACE key.

Allowed features are displayed in green, blocked features are displayed in red.

5.5.1. User Variables

Application Possibilities for user variables

If user authorization is active, user variables can be used in the following fields in the eLux control panel.

Configuration (Applications)

Option	Function	User Variable
Shut down > Lock	Manual activation of the screen saver lock	Preset with the value of $ELUXPASSWORD

Setup Tab (Setup)

Option	Function	User Variable
Drives	User name	$ELUXUSER
	Password	$ELUXPASSWORD
	Directory, Server, Share	Every $ELUX-Variable
	Browser home directory	Every $ELUX-Variable
Screen	Screen saver password	$ELUXPASSWORD

Configuration Tab (Configuration)

Option	Function	User Variable
ICA/RDP	Server	Every $ELUX-Variable
	User name	$ELUXUSER
	Password	$ELUXPASSWORD
	Domain	$ELUXDOMAIN
Browser	Proxy, Proxy-Port	Every $ELUX-Variable
Tarantella	Server	Every $ELUX-Variable
Local customized commands	Parameter Application possibility: Programs that can be executed by using the command line. For example: `rdesktop -u $ELUXUSER -p $ELUXPASSWORD <machine>`	Every $ELUX-Variable

Setting new user variables

For using User Variables you have to activate the FPM **LDAP search module** (usersearchldap) in the EPM **User authorization modules** (userauth). By default this feature package is not activated.

Predefined User Variables are: $ELUXUSER, $ELUXDOMAIN and $ELUXPASSWORD.

1. Choose via the drop down menu a type of access authorization.
2. Click **Edit**.
3. Choose **User Variables**.

4. Edit the following fields:

Option	Description
Local variable	Enter a name for the variable. The name must begin with the prefix “ELUX” without the initial “$”. End with the “#” character to transfer more than one value, for example, ELUXMAIL#-#=mailLocalAddress. If more than one mail account address resides on the server, they will be transferred using the nomenclature ELUXMAIL_1, ELUXMAIL_2, etc. In this case, the variable ELUXMAIL_0 contains the number of mail addresses that were read.
LDAP variable	Enter the name of the attribute that the LDAP or Active Directory should assign the variable. As an example, the LDAP/Active Directory schema can contain the attribute “displayName”. If you assign this attribute to the variable ELUXFULLNAME, it will be assigned the value of this attribute during the next user authorization call.

5. Click at **Test**.
   Now the thin client attempts to retrieve from the authorization server the value for the attribute you already entered.
6. Click at **OK** in the window **User Variables** and **Apply** in the field **Security**.

5.6. Firmware

In the **Firmware** tab you can change settings for the firmware update (software update) of the clients via network.

5.6.1. Requirements

- Web-Server (like IIS), which provides the eLux Software packages and Image Definition Files via HTTP or FTP.
- Software container with eLux software packages on the web server (installation component of the bundles eLux[version]_AllPackages.zip von www.myelux.com)
- ELIAS tool (eLux Image Administration Service) to create and modify Image Definition files in the software container on the web server (component of the Scout Enterprise-Installation)
- Scout Enterprise console to configure firmware updating for the clients (component of the Scout Enterprise-Installation)

5.6.2. Configuring firmware update

In **Setup > Firmware** you can configure firmware updating of the clients via network using the following options:

Protocol	Network protocol of the web server for software package transfer to the clients (HTTP, HTTPS, FTP, FTPS)
Server	Name (FQDN) or IP address of the web server containing the eLux software packages and the Image Definition Files
Proxy	(optional) IP address and port (fix 3128) of the proxy client Syntax: `IP-Adresse:Port` Example: `192.168.1.100:3128`
User	(optional) User name for access to the eLux-Software-Container of the web server. If there is no explicit user name, use `elux`.
Password	(optional) Password for access to the eLux-Software-Container of the web server. If there is no explicit user name, use `elux`.
Pfad	Directory path of the eLux software packages on the web server-Pakete auf dem Web-Server. Please use slashes `/` as separators. Example: `eluxng/UC_RP` corresponds to the IIS web server directory `C:\inet-pub\wwwroot\eluxng\UC_RP\` If running devices with both, eLux RL and eLux RP, you can replace the container name `UC_RP` by the container macro `__CONTAINER__`. The clients resolve the container macro according to their installed eLux version to `UC_RL` or `UC_RP`, respectively. The advantage involved is using only one Image Definition file name for the two IDFs that have been defined for eLux RL and for eLux RP in ELIAS.

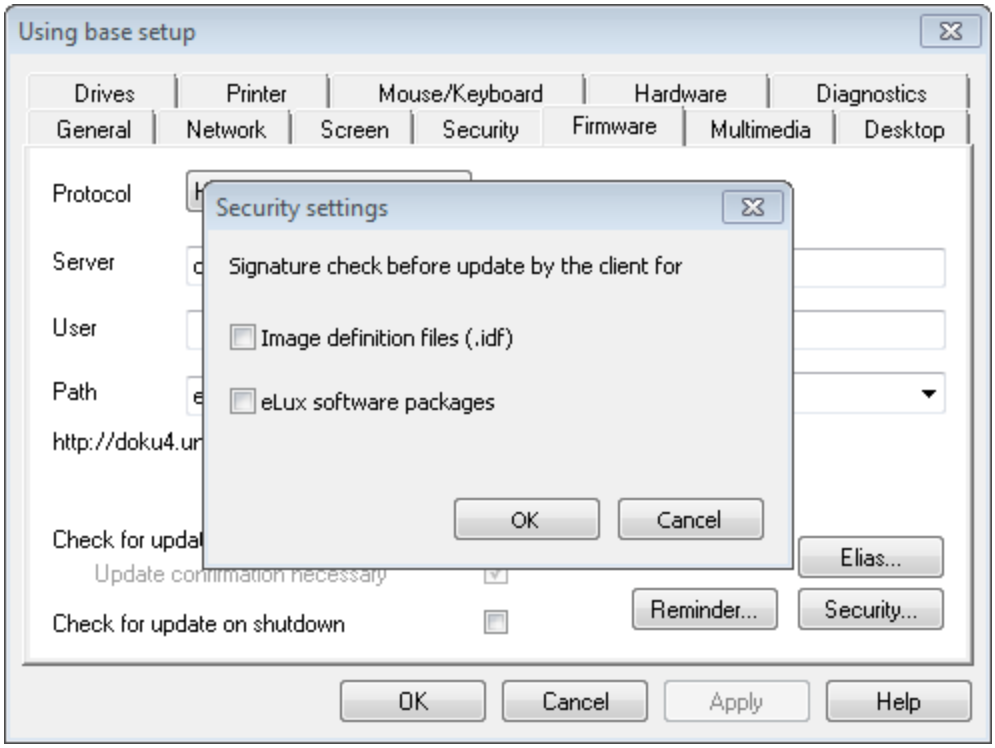
Note
The admin can replace the container macro name by a fix container name. In this case the entry in the **Path** field must correspond to the actual container name on the web server.

Image file	Name of the Image Definition file (IDF) on the web server, which should be used for firmware updating by the clients. Do not use spaces.The file name is case-sensitive and requires the file extension `.idf`. Example: `myImage.idf`
	Note The fields **Protocol**, **Server**, **Path**and **Image file** are used to build an URL-address, which is used by the clients when starting the transmission of Image Definition file and eLux software packages for firmware update. The URL address is displayed below of the **Path** field.
Check for update on boot / shutdown	The Thin Client checks during boot or shutdown, if there are firmware updates available and necessary. You can set the option **Update confirmation nesessary** to let the user decline the update, if required..
Elias... button	Starts the ELIAS tool and opens the Image Definition file indicated in the **Image file** field.
Security... button	The **Security settings** let you define signature check before update through the client.Signature check can be performed for the Image Definition files and/or for the eLux software packages.
Reminder... button	The **Reminder Settings** let you define if a user can defer a firmware update and how often he can do. Moreover you can specify time intervals for the update reminder. For more information, see Update deferment through user.

5.6.1. Security – Signature check before update

You can configure Scout Enterprise to make the client check signatures each time before an update is performed. In this case an update is performed only if the signature of the Image Definition file (IDF) and/or the signature of the eLux software packages have been verified successfully. The update can't be run, however, if the IDF or one of the eLux software packages to be installed, do not have a vaild or verifiable signature.

Activating signature check



1. In **Setup > Firmware**, click t **Security...**...
2. Under **Signature check before update**, check the **Image Definition file** option and/or the **eLux software packages** option.

*The result of the signature verification is documented in the update log file on the client. After having performed an update, the update log file is sent to Scout Enterprise server and can be viewed for the selected device in the **Properties** window by double-clicking the **Update status** field.*

Verifying the IDF signature on the client side requires the root certificate, but also the signature certificate in the local client directory /SETUP/CACERTS. If you use own certificates for signing IDFs or individually composed eLux packages, you can configure them using the Scout Enterprise command **Options > Advanced options... > Files**. For those eLux packages provided by Unicon, all needed certificates come along with BaseOS eLux RP 4.7.0 or higher.

How to create IDF signatures, see Signing an IDF in the ELIAS guide.

Note

Signature check of eLux software packages requires an update partition on the client computer.On devices that have no update partition, signatures can only be checked for Image Definition files but not for eLux software packages.

Beginning with eLux RP 4.6.1 an update partition is created automatically for devices having 2 GByte or more flash memory when performing a recovery via PXE or USB stick or when performing a firmware update including flash formatting before update.

5.6.1. Update deferment through user

This feature gives the user the chance to determine update time himself, when the administrator uses the **Update** Online command. The user can avoid firmware updates while using the client.

The client reports the current update process status to Scout Enterprise server. The status can be viewed in Scout Enterprise console in the **Update State** field of the relevant **Properties** window.

Moreover you can use the Report generator to evaluate the **Update State** field by the value `Deferred` (other: `Succesful`, `Not succesful`, `Not necessary`).

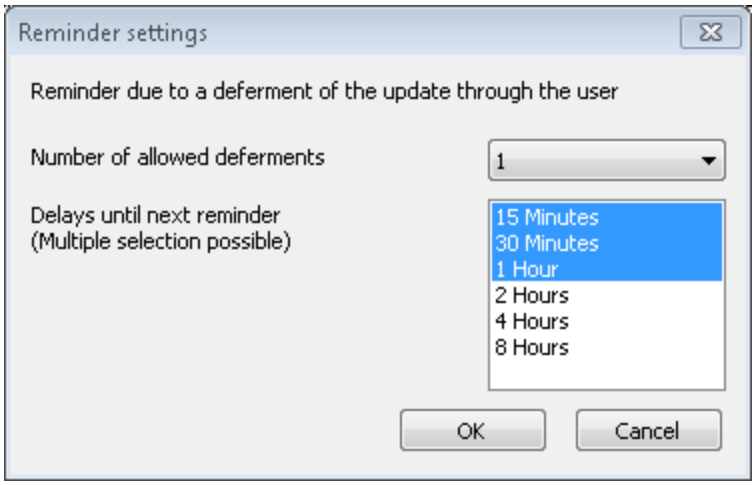
Important
Update deferment must be configured once on the **Firmware** tab and, secondly, it must be enabled for any Update Online Command you run.

Configuring deferment of firmware updates through the user

1. In the **Setup > Firmware** dialog, click **Reminder...**

   *The **Reminder settings** dialog opens.*

2. Select the **Number of allowed deferments** in the list.
3. In the **Delays until next reminder** list, click one or more time intervals from which the user can select the delay for the next reminder.



The possibility of update deferment for the user is enabled. If the admin configures the next Update Command as follows, the user will get a system message including a deferment option.

Enabling deferment in an Update command

1. On the context menu of an OU or device, click **Commands > Update...**

   *The **Execute command** dialog opens.*

2. Check the **Inform user for** option .

*This option triggers the system message to be shown at the client and gives the user the chance to control the time of the update process. If the **Number of allowed deferments** in the **Reminder settings** is set to `1` or more, the system message provides the option for the user to postpone the required firmware update.*

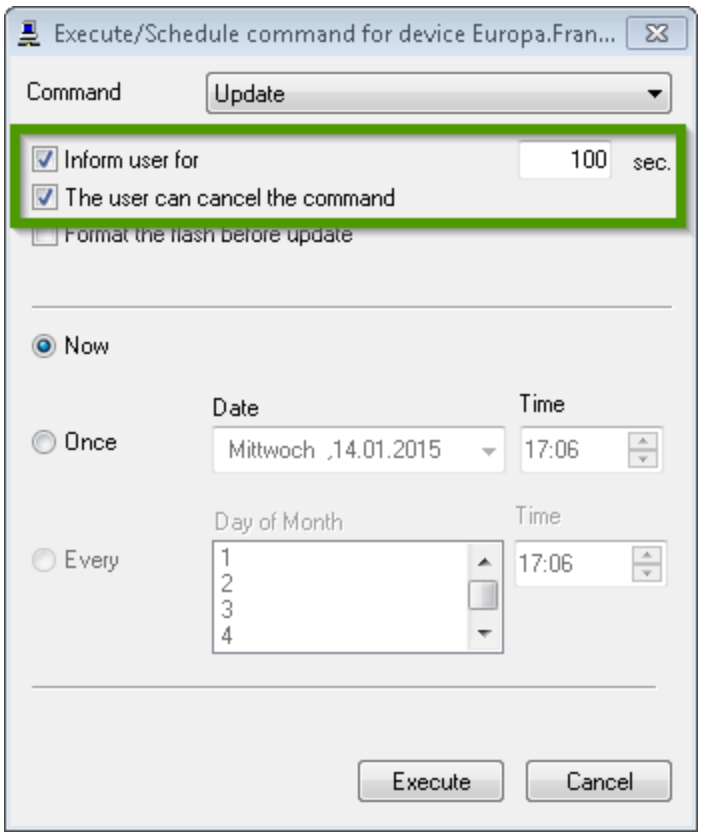
3. In the box next to **Inform user for**, enter the display duration of the system message in seconds.

   *Within the defined time period the user is given the chance to close applications and to log off before updating. In addition, the user is given the chance to defer the firmware update for a selectable interval (as defined in **Delays until next reminder**).*

   If you leave the display duration at `0`, the system message will be shown until the user clicks one of the push buttons.

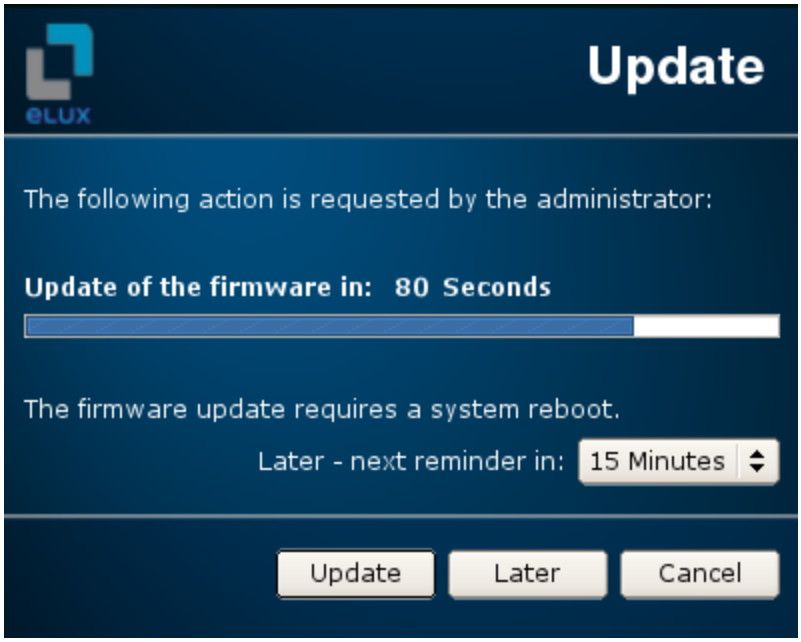
4. If desired, check the **User can cancel the command** option .

   *The system message on the client will contain a **Cancel** button. The user is enabled to abort the firmware update definitely, there is no self-acting retry of the update process.*



System message announcing firmware update on the client

Any **Update** command with user information specified provokes a system message including the defined options for the user:



Element	Description
Later - next reminder in	Select list containing the time intervals for the next reminder of the firmware update, defined in **Delays until next reminder**. Is displayed only, if the **Number of allowed deferments** is set to `1` or higher, and if at least one more deferment is possible.
Update button	Perform firmware update immediately.
Later button	Postpone firmware update by the time period selected. If the client is shut down before timeout, the update is performed during shut-down. Is displayed only, if the **Number of allowed deferments** is set to `1` or higher, and if at least one more deferment is possible.
Cancel button	Abort update process definitively. Is displayed only, if the option **User can cancel the command** is checked.

5.7. Multimedia

The following sound settings are available:

- The controllers **Total**, **PCM** and **Microphone** adjust the sound level for playback and recording.
- For the microphone, the **Mute** option prevents the recorded sound from being played back on the audio out port. The option **Mute** is active by default in order to avoid noise. When the mic is muted and you use a headset, the recorded sound on the headphone will not be played back but it will still be recorded.
- To switch off the microphone recording you must move the Microphone silder down to `0`.
- If the **system beep** is activated, the system provides an acoustic response signal while switching off the thin client.
- If **audio in XDMCP** is activated, sound can be rendered in a session by using a X-server.

5.8. Desktop

Modify in this tab the design of eLux desktop surface and configure calendar date and time zone.

5.8.1. Configuring desktop

1. In Scout Enterprise for the relevant device or OU open **Setup > Network**. The same dialog works for eLux on the client.
2. In the **Language** list, click the preferred application language.

> **Note**
> To ensure correct performance, the applications have to support the selected language.

If you select `German`, the eLux user interface elements such as start menu and control panel will be displayed in German. If you select any other language they will be displayed in English.

3. Click the **Background color** button to select a background color.

> **Note**
> The selected background color comes only into effect, if the option **Classic Desktop** is checked, see Advanced desktop configuration.

4. In the **Task Hotkey** list, select a shortcut to switch between the sessions.

   The default is `ALT+CTRL+↑` to avoid any conflict with the shortcut `ALT+TAB` which is used to switch between the tasks within one session.

5.8.1. Adjusting calendar date and time zone manually

1. Adjust the calendar date and the time zone via the corresponding fields.
2. Confirm with:**Synchronize**.

5.8.2. Advanced desktop settings

In **Desktop > Advanced** the following options are available:

Option	Description
Theme	Defines a desktop theme, from RP on no more available.
Interactive Desktop	Defines the icons to be be displayed on the desktop.
Desktop writable	Defines whether users are allowed to place icons on the desktop.
Classic Desktop	Deactivates the eLux Modern User Interface. Only then the **Background colour** chosen on the **Desktop** tab will be active.
Window manager	If the option **Animated Windows**is active the windows' content is displayed while moving them. If the option **Maximize/Fullscreen** is active, you can assign a particular monitor to an application (ICA and RDP).
Task bar	Settings for the task bar at the bottom of the screen.

Option	Description
Quick Setup (Systray)	Defines the systray icons to be displayed in the task bar. **Multimedia**: Selecting input and output devices, Volume control, Test sound **Mouse/Keyboard**: Mouse and keyboard speed, left-handed mouse, keyboard language **Screen**: Information, resolution, alignment **USB mass storage devices**: Information about USB devices **Show network status**: LAN/WLAN, network information, disconnect/connect, configuration **Device information**: MAC, IP, name, serial number, free information fields **Date/Time**: Display and configuration of date, time and time zone
Background image	In Scout Enterprise you can define background images. There are two ways: • Enter the picture file name including its path relative to the Scout Enterprise Server directory (`...\UniCon\Scout\Server`) into the field **Server file**. • Click **Load** to browse and select the picture file. The picture file will be imported into the database. This option has precedence over a file referenced in the file system.. Click **Delete** to remove the current background image from the database.
	Note Files that you import into the database will be saved with the SQL database backup. Files that you reference in the file system provide the opportunity to be replaced by other content as long as the file name does remain.
	The background image is not reloaded with every boot routine, but only after changes have been made in file configuration or in the files themselves. eLux NG does not support desktop wallpapers and stacked images.
	Note Make sure to have enough space on the client flash card. The background image is stored in the `/setup` directory of the flash card.
Autostart	Defines if the control panel should be started with system start and defines the delay in seconds.
Work spaces	Defines the number of desktops.

5.9. Drives

5.9.1. General

In this tab you define the connections to drives and there is also the possibility given to indicate a drive where browser data can be saved.

5.9.2. Establishing a network drive

1. Click at **New**
2. Type the following information into the fields:

Information	Description
Directory	Name of the directory. eLux automatically adds '/smb/. The data is local at the directory '/smb/<Name of directory> available.
Server	Name of the server
Share	Enter the name of the windows drive share.
User name and password	Enter the user name and the corresponding password which you also use for signing in to the server.
Active Directory Authorization	Enables logon via Active Directory. In this case the fields user name and password will be disabled.

3. Click **OK** and **Apply.**

5.9.3. Defining the browser home directory

If you define a browser home directory, browser settings will be saved on a mapped network drive to make them available after reboot.

If you don't define a browser home directory, the settings will be lost after reboot.

5.9.4. Mount points

Mount points are used to access local ressources through an application. The following mount points are provided by eLux:

Samba	`/smb`
NFS	`/nfs`
internal CD-ROM	`/media/cdrom`
USB devices	`/media/usbdisk*`

*For USB devices the mount points are assigned chronologically: The first device gets `/media/usbdisk`, the second one gets `media/usbdisk0` and so on.

Mounted devices are shown in the systray if the option **Desktop > Advanced > Taskbar** is enabled.

Due to security reasons, the **USB interfaces for mass strorage devices** must be checked on the Hardware tab

Note

Drive mapping to access local resources has to be defined in the relevant application definition. For Citrix ICA application see ICA software defaults, for RDP application see Advanced RDP settings.

5.10. Printer

5.10.1. General

The eLux print service supports printing from local applications both to locally connected printers and to network printers. In addition, other workstations or servers within the network can use a locally installed printer on a thin client running eLux. The printer has to support LPR and TCP direct print.

In Scout Enterprise **Setup > Printer > New** you can define and configure local printers with logic names. These printers can be accessed within the network.

The option **Print service** makes the print service start on the client.

5.10.2. Selecting printer as standard printer

1. In Scout Enterprise for the desired OU or device, open **Advanced settings > Printer**.
2. In the **Default printer** list, select the printer that you want to be the default printer.

   The list provides all defined printers.If the desired printer is not in, you have to define it on the **Printer** *tab of the base configuration or of a parent OU first.*

5.10.1. Defining a network printer

1. Enable the Windows LPD service (Line Printer Demon).

   The TCP/IP printer service will be installed and started. The service is required to address the printer.

2. In Scout Enterprise-console, open the **Setup** dialog:

All devices	**Options > Base configuration... > Printer**
All devices of a particular OU including subordinate OUs	context menu of OU and **Setup... > Printer**
Single device	context menu and **Setup... > Printer** or on the client in the control panel **Setup > Printer**

3. Click **New**.

   The ***Define printer*** *dialog opens.*

4. Enter a **Name** for the network printer.
5. In the **Connection type** list, click `Network`.
6. In the **Filter** list, click one of the following options:

Option	Description
None	Enables printing from a remote session. Printing data from the session are forwarded to the printer in unfiltered RAW format. The printer driver name has to match the name in the server's drivers list(case-sensitive).
Text	Enables printing from a local shell.

Option	Description
PCL2	Enables printing for web sites and PDF files opened with the local Firefox in eLux.. The connected printer must supportthe language **PCL2**, **PS** (Post-script) or **PDF**.

Note
If a printer is defined on the client, you can print in different scenarios. For example, you can print text from a local shell or a PDF file out of eLux' Firefox browser. Furthermore, you can print from a remote session. When printing from a Citrix session, the filter `None` will be used automatically . Hence eLux is able to send the preprocessed data directly to the defined printer. For more information, see Citrix auto-created printers in the Scout Enterprise Manual.

7. In the field **Printer address** enter the IP address of the server.
   Or:
   Enter a host name from the local host file on the client in **Setup > Network > Advanced**.
8. In the field **Printer queue** enter the share name of the printer.
9. In the field **Driver name** enter the printer's driver name.

Important
Make sure that the printer driver name is identical to the one of the printer installed on the server.The name is case-sensitive and sensitive to blanks. If the names do not match, the server will not identify the driver.

10. Confirm with **OK**.
11. In the **Setup** dialog confirm with **Apply**.

5.10.1. Citrix auto-created printers

Citrix XenApp provides automatic configuration of printers (dynamic printer mapping) That means, when logging in via ICA an automatic printer definition on the XenApp server will be created. This printer definition is valid only for the duration of the ICA session. After closing the session the definition will be deleted. It can only be used by the logged-on user.

XenApp can auto-create local printers connected on the client device or a generic printer, the Citrix Universal Printer, which is not tied to any specific device.

Configuring local printer for auto-creating on the client:

1. In **Configuration > Printer**, specify one ore more printers.
2. In the **Define Printer** dialog, in the **Name** box, enter the Microsoft Windows printers name exactly in the same way it is in the drivers list of the server.The name is case-sensitive.

When the user starts an ICA connection to the Citrix XenApp server, he can see icons for the automatically created client printers in the **Start > Settings > Printer** *dialog with*

`Client\`*<Hostname>#\<Printer>*

<Hostname> is the hostname of the thin client and <Printer> is the name of the printer defined in Scout Enterprise.
If the specific driver is not installed on the application server or the name is not identical, the client printer can not be created. In this case the universal printer will be used.

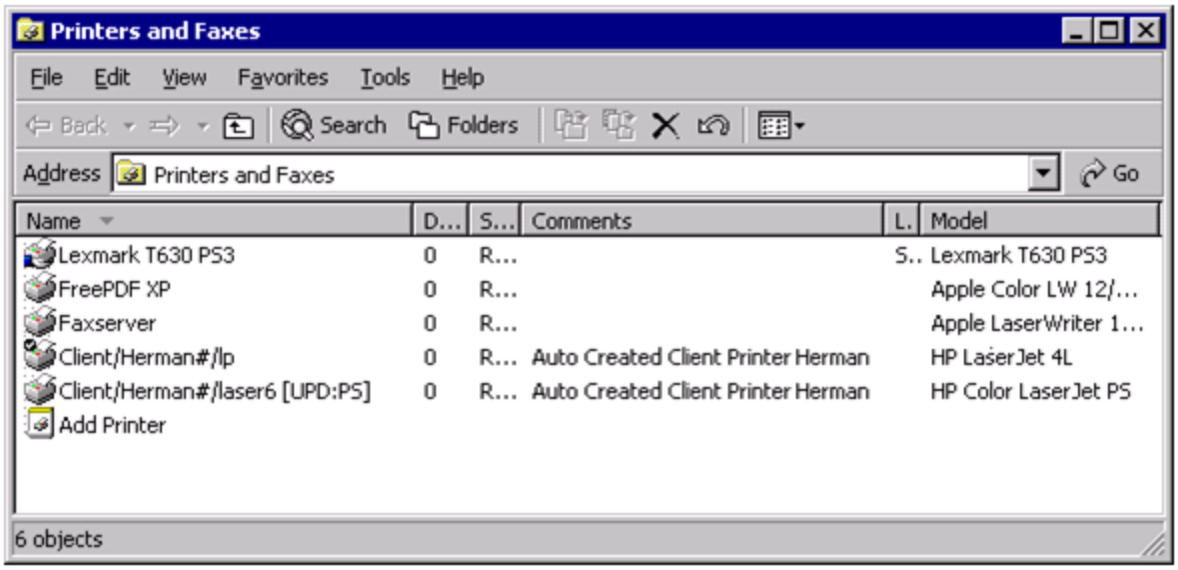
Configuring Universal Citrix Printer on XenApp server

This feature requires the current Citrix ICA client for Linux. The generic driver is the XenApp universal driver.

1. Sign in as administrator on the XenApp server.
2. Open the management console for XenApp.
3. On the context menu of **Printer Management**, click **Properties**.
4. In the left-hand panel, click **Printers**, and then configure the auto-creation of client printers. For more information, see the Citrix documentation.
5. In the left-hand panel, click **Drivers**, and then configure the driver:

Setting	Description
Native drivers only	A client printer will be created by using the native printer driver defined in Scout Enterprise. If this driver is not installed on the XenApp server, the client printer won't be created.
Universal driver only	A client printer will be created. The printer driver defined in Scout Enterprise will be replaced by the generic driver.

Setting	Description
Use universal driver only if native driver is unavailable	A client printer will be created by using the native printer driver defined in Scout Enterprise. If the native driver is not installed on the XenApp server, the generic driver will be used.
Both universal and native drivers	Two versions of each client printer will be created, one supported by the generic driver and one supported by the native driver already defined in Scout Enterprise.
Automatically install native drivers for auto-created client and network printers	Native printer drivers will automatically be installed on XenApp servers if **Autocreation** is active.


Printers and Faxes
File Edit View Favorites Tools Help
Back Search Folders
Address Printers and Faxes
Go
Name D... S... Comments L. Model
Lexmark T630 PS3 0 R... S.. Lexmark T630 PS3
FreePDF XP 0 R... Apple Color LW 12/...
Faxserver 0 R... Apple LaserWriter 1...
Client/Herman#/lp 0 R... Auto Created Client Printer Herman HP LaserJet 4L
Client/Herman#/laser6 [UPD:PS] 0 R... Auto Created Client Printer Herman HP Color LaserJet PS
Add Printer
6 objects

If a universal printer driver is used, the text

`[UPD:<generic driver name>]` is appended to the printer name, where <generic driver name> is `PS` in the example.

In the figure above, the client printer `client/Herman#/lpis` created using the native driver `HP LaserJet 4L` and `Client/Herman#/laser6` is created using the generic driver for PostScript, as the specified driver `HP LaserJet PS` is not installed on the application server.

For detailed information on server-side settings for universal drivers, see **Citrix Product Documentation** for XenApp.

5.10.1. Using TCP direct print

In TCP direct print, data is sent directly to the printer. There is no spooling of print jobs on the Thin Client and the data are not modified before printing. The flow is controlled by TCP/IP.

- Enter at the print server the IP address of the particular thin client, printers name and the port number

5.10.2. ThinPrint

ThinPrint® software from ThinPrint GmbH in Germany allows optimized network printing across various platforms. The software consists of a server component and a client component. The ThinPrint server processes and compresses print data for the target printer and sends it to the client. The ThinPrint client receives the print jobs from the server, decompresses them and sends them to the selected printer. ThinPrint server and client are connected via TCP/IP. Unlike TCP direct, LPR or CUPS, ThinPrint is a print protocol that allows you to specify the bandwidth. Therefore it is suited for networks with small bandwidth.

Configuring ThinPrint

1. Install the ThinPrint client on the Thin Client.
2. Connect the desired printer.
3. If you use Windows CE clients, in the **Setup > Printer** dialogue at **Thin Print** select the relevant protocol.
4. In **Setup > Printer > New**, define the printer and under **ThinPrint** check the **thinprint** option. Optionally enter a class name of up to 7 characters.
5. Configure the ThinPrint server. For more information, see the ThinPrint® documentation on www.thinprint.com.

5.10.1. CUPS

General

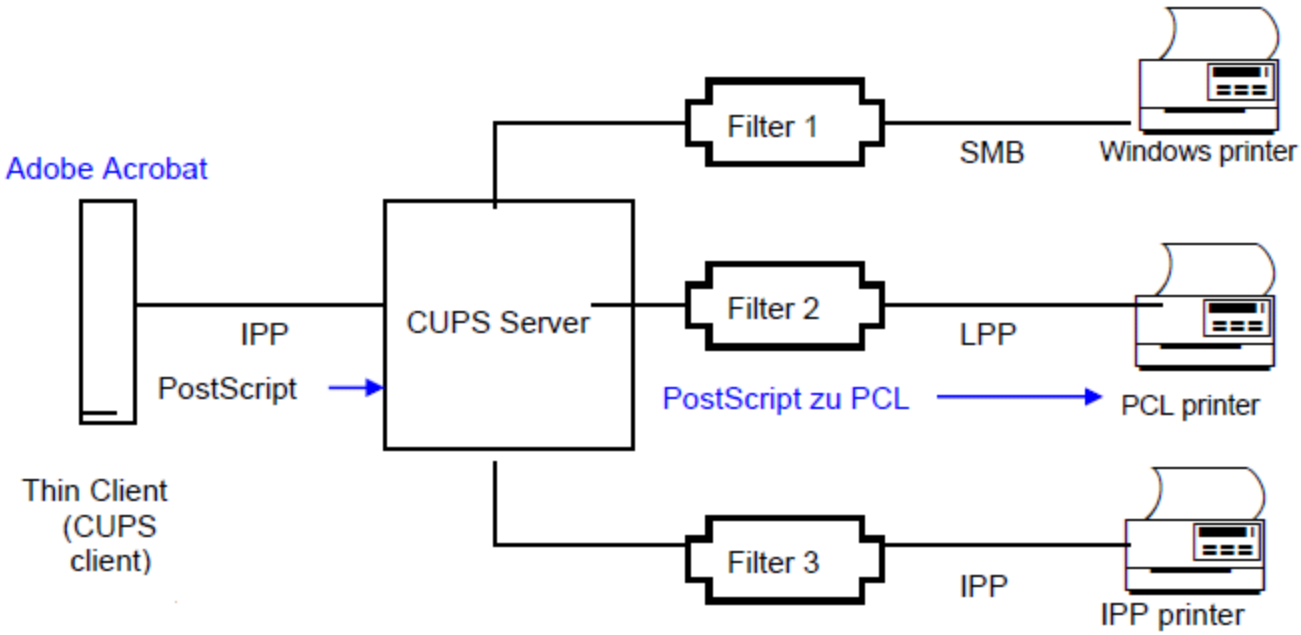
The Common UNIX Printing System™ (CUPS™) is a software solution from Easy Software Products. It provides a common printing interface within a local network and dynamic printer detection and grouping. The advantage of CUPS is that all configuration takes place on the CUPS server. No configuration takes place locally on the client.The CUPS server contains a list of back-ends, including parallel port, USB connections, serial connections and network (LPD).

On the thin client, when the CUPS client is installed, it replaces the local LPD printing system. All local printer definitions in Setup > Printer are ignored.

The CUPS client and server are provided free of charge. Commercial add-ons and support for the CUPS server can be purchased from Easy Software Products.

CUPS is used to print from local applications on the thin client (for example, Adobe Acrobat or a local browser). These local applications have PostScript as output format. If you do not have a PostScript printer, you must install a filter (for example, PostScript to PCL) on the CUPS server.

CUPS procedure



1. Adobe Acrobat generates the output file (PostScript format) and sends it to CUPS server via IPP.
2. CUPS converts PostScript to PCL by using preinstalled filter.
3. CUPS sends print job to printer using preinstalled backend (parallel, serial, network etc.).

Configure CUPS on the thin client

1. Install the CUPS server on a computer of your choice and configure the CUPS server.
2. For information on how to install and configure the CUPS server, please visit www.cups.org.
3. A guidance for installing and configuring the CUPS server can also be found at www.cups.org.

4. Define the environment variables in Scout Enterprise as follows:

Option	Description
CUPS_SERVER	Host name or IP address of the CUP server.
CUPS_OPTIONS (optional)	Allows you to preset user-dependent print options. These options are defined in the printer's *.ppd file. Contact a CUPS administrator for this value. For example: CUPS_ OPTIONS=-o OutputBin=Bin2. **Tip:** In the case you use LDAP or ADS, in place of the environment variable CUPS_ OPTIONS set in Scout Enterprise you can use the user variable ELUX_PRINTEROPTIONS set on the LDAP or ADS server.

5. Adopt the environment variables on the thin client.

Printing from a local browser

1. Start Firefox.
2. Open a website that you want to print from.
3. Click **File > Print**.

   The browser's **Print** *dialog opens.*
4. Leave the settings and click **OK**.

   The CUPS dialog **Print** *opens.*
5. In the **Name** list, select a printer (the provided printers depend on the server-side settings).
6. If required,edit further settings.
7. Click **OK**.

   The printing process starts.
8. After printing, click **OK** to close the **Print information** dialog .

5.11. Mouse/keyboard

5.11.1. Configuring mouse settings

1. On the **Mouse/Keyboard** tab, under **Mouse** , select your Mouse type or `Auto`.

   Normally, the type of the mouse is recognized automatically.

2. Under **Double click speed**, move the slider to the right to increase the speed.

   Double click speed defines the time interval between the two clicks to be identified as a double-click.

3. Under **Acceration**, move the slider to the right to increase acceleration of the mouse pointer.

   The faster the mouse pointer, the smoother the movements.

5.11.1. Configuring the keyboard

1. On the **Mouse/Keyboard** tab, in the **Language** list, select a language.
2. In the Type list, leave `Auto`.

   The type of the keyboard is recognized automatically.

3. Under **Delay**, move the slider to the right to increase the delay.

   Delay controls how long a key needs to be pressed until the letter will be retyped.

4. Under **Speed**, move the slider to the right to increase speed.

   Speed controls how fast a letter will be retyped while a key is pressed.

5.11.1. Advanced mouse and keyboard settings

1. On the **Mouse/Keyboard** tab, click **Advanced**.

Option	Description
3 button emulation	In general, eLux is used with a three button mouse. However, it is possible to achieve the same functionality with a two button mouse. A third button is simulated, when the user presses the left and right mouse buttons simultaneously.
Left-handed	Reverse mouse buttons.
Dead Keys	Dead keys make it possible to enter accented combination characters. A dead key combination means that you press two keys one after the other (press the first key and release it, then press the second key and release it) in order to form a single character. In general, you press a key for the accent you want (nothing happens), then a key for the letter to apply to accent to (the accented combination character appears). By default, dead keys are active. If you use an application which is incompatible with dead keys, clear the option. Note: Some hardware platforms do not provide this option.
Numlock	Deactivates NUM during boot procedure of the client. By default, NUM is active.

Option	Description
Console switch enabled	Allows the user to switch between consoles by using hotkeys. By default, this option is checked. Using CTRL + ALT + F4 or CTRL + ALT + F1, respectively, the user can switch to the command shell and back. If the option is not checked, console 1 and the eLux desktop are always shown. For more information, see Shortcuts.
Enable extended keys	Enables multimedia keys and other keys with special functions on the keyboard.

2. Click **OK** to confirm.

The modifications will be active on the next reboot of the thin client.

5.12. Hardware

5.12.1. USB mass storage devices and card readers

The checkbox **USB mass storage devices** defines whether or not USB mass storage devices can be connected. The checkbox **inform user**defines whether a pop-up window appears in the event of connection an USB mass storage device. Via the dropdown list you can choose if a card reader should be activated.

5.12.2. USB rules

The syntax of the USB rules corresponds to the Citrix USB guidance rules. Use the **Device configuration / hardware** tab to define the rules.

Note

Using the USB rules, deactivates the **Hardware > USB-mass storage devices** option valid for thin clients from eLux RP version 4.1 or higher. Clients equipped with older software versions do not evaluate the USB rules, but the **USB mass storage devices** option. To support mixed client versions, the **USB mass storage devices** option remains changeable even when USB rules are activated.

Manufacturer ID (VID) and product ID (PID) can be found in **USB device info** in the task bar.

Example rules:

Rule	Code
Allow a specific USB mass storage device model only	`ALLOW: VID=0781 PID=5151` # USB-Stick-Modell erlauben (z.B. SanDisk Cruzer Micro) `DENY: CLASS=08` # Deny all devices of the class MASS STORAGE DEVICES.
Deny a specific SmartCard model only	`DENY: VID=18a5 PID=0302` # SmartCard-Modell verweigern (z.B. Omnikey CardMan 3821) `ALLOW: CLASS=0B` # Allow all devices of the class SMARTCARD
Deny all printers, mass storage devices, SmartCard readers.	`DENY: CLASS=07` # Deny all devices of the class PRINTERS `DENY: CLASS=08` # Deny all devices of the class MASS STORAGE DEVICES. `DENY: CLASS=0B` # Deny all devices of the class SMARTCARD.
Deny all devices	`DENY:` # Deny all devices.

Attention

The USB rules influence all USB devices classes and therefore also the class HID (Human Interface Devices). If you deny Class 03 HID it will deactivate mouse and keyboard. A denial of all classes (DENY: # deny all devices) influences internal USB hubs and devices of manufacturer specific device classes, for example WLAN modules, on the client. By using particular hardware combinations there might be problems during boot process of the client. We recommend you to execute tests before you finally use this option.

5.13. Diagnosis

Using the **Diagnosis**tab you can enable or disable enhanced debugging on the client.

If the **Debug level** is active, the feature **Device diagnosis** helps you run predefined commands on the client and retrieve a set of configuration and log files.

If you require technical support from Unicon, switch on enhanced debugging before you perform **Device diagnosis**.

Device diagnosis is performed using an online command, for more information, see Device diagnosis.

Note
Make sure to switch off debugging mode after having performed device diagnosis. Otherwise you risk to exceed memory capacity of the thin client.

5.14. VPN

5.14.1. Unterstützte VPN-Clients

Abhängig vom eingesetzten Thin Client Betriebssystem werden die folgenden VPN Clients unterstützt:

- F-Secure
- FreeS/WAN
- Cisco VPN Client
- PPTP VPN Client
- VPNC VPN Client
- L2TP VPN Client
- Juniper

6. Advanced settings

The settings of the device configuration that you have defined in the base configuration or for particular OUs or devices, respectively, can be

- overridden for particular devices or OUs
- extended by further specific options

using the **Advanced settings**.

Opening Advanced settings

- In Scout Enterprise menu click **Options > Advanced settings** to override or to add settings for all devices.
- For the relevant OU or device open the context menu and click **Advanced settings...** to override or to add settings for this OU/device.

*The **Advanced options** dialog contains the following tabs:*

- Devices
- Update
- Wake On LAN
- Files
- Advanced file entries
- Rules

6.1. Devices

Note
The **Devices** tab is only available for the global **Advanced settings** which are called via menu **Options > Advanced settings**. These settings will be applied to all devices.

1. In the **Advanced settings** dialog, click the **Devices** tab.
2. Edit the following fields:

Option	Description
Maximum pingtime (milliseconds)	Defines the pingtime of a particular thin client.
Maximum search time (seconds)	Defines the time period for searching thin clients.
Only locked fields are updated on the client.	Editable fields will not be overwritten by Scout Enterprise. Thus the end user can define individual settings such as screen resolution and the setting will not be overridden even though Scout Enterprise modifies other parameters. If a user defines a setting which is noct supported by the client, for example a too high screen resolution. Scout Enterprise can reset the client to factory state and the client gets assigned all parameters again. As soon as the new configuration is loaded, the locked fields in **Setup > Security** will be updated, the values of the other fields remain as defined by the user.
Default OU	Defines the OU in which new devices will be assigned by default.
Assign OU depending on OU filter	Activates the OU filter for new devices. By clicking the **...** button you can configure the OU filter.See Setting up an OU filter.
Name template	Choose a name template. According to this template the currently added clients are to be named.
Deactivate new devices	Deactivates the shortly added devices.

3. Confirm with **OK**.

6.2. Update

1. In the **Advances settings** dialog, click the **Update** tab.
2. Define the **maximum number of parallel updates**to be performed simultaneously.
3. In the field **Maximum time to connect** define the time period for connection build up.
4. Confirm with **OK**.

Note
The optimum values depend on the system.

6.3. Wake On Lan

Defining a Wake On LAN server is optional. Wake On LAN remotely controls (turns on) all thin clients within its subnet. This is useful for remote subnets, but is not required for the local subnet where Scout Enterprise is located. A Wake On LAN server is included on the CD-ROM.

A Wake On LAN server can either be set globally, or for an individual device, for a group or a specific location.

1. In the **Advanced settings** dialog, click the **Wake On LAN** tab.
2. Edit the following fields:

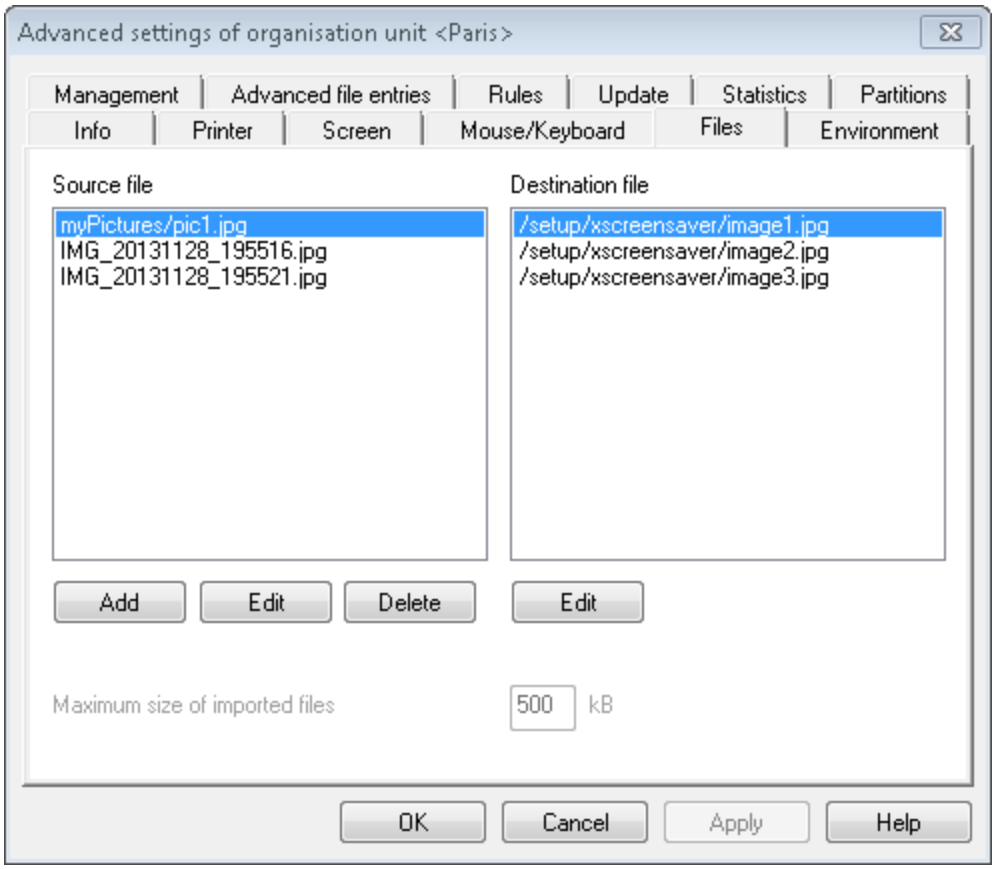
Data	Description
Server name	The entered Wake On LAN IP address in this field is used as the standard IP address for all devices. For using a client equipped with eLux as Wake on LAN server for other eLux clients use the format: `eLux < IP address.`
Generate an IP broadcast address for the subnet.	The packet will be sent to the subnet the device belongs to (dedicated subnet). Enter the subnet address in the **Server name** field using the format `/255.255.255.0`. Note the leading slash. Example: To wake up a device with IP address `192.168.10.44`, enter `/255.255.255.0` in the **Server name** field. The broadcast address which is entered in the packet is `192.168.10.255` This option is not checked by default.

3. Confirm with **OK**.

6.4. Files

This feature helps you transferring files to the client. You can define files to be transferred on the next reboot for all devices, for a single device or the devices of an OU.

The source files can be referenced in the file system or imported to the Scout Enterprise database.



Example: You might wish to copy one or more picture files to the clients to be used as screen saver.

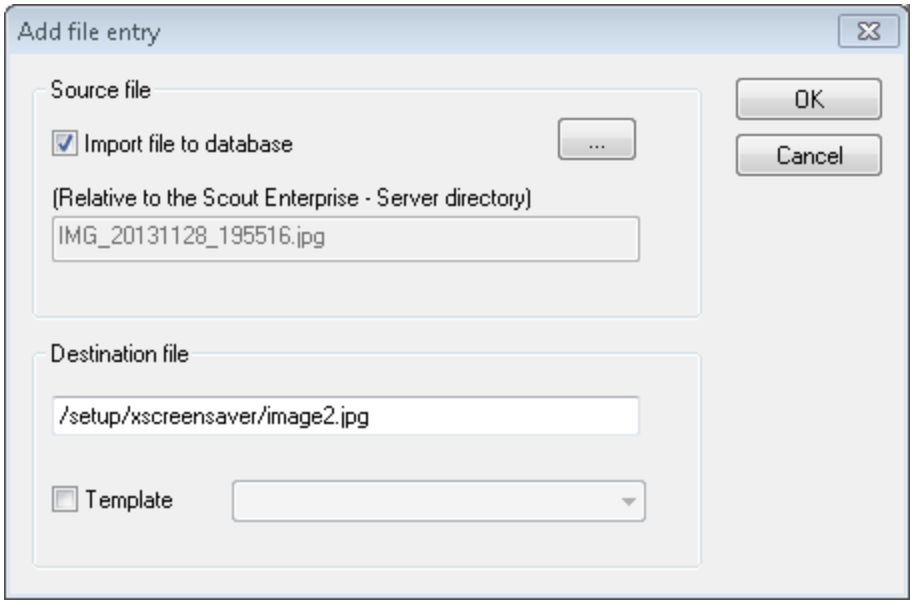
Defining files for transfer

1. If you want to configure file transfer to all devices (global file list), click **Options > Advanced Settings...**.
   If you want to configure file transfer to the devices of a particular OU or to a single device (individual file list), open the context menu of the relevant OU or device and click **Advanced settings...**

> **Note**
> Individual file lists have precedence over global file lists.

2. Click the **Files** tab.
3. Click **Add**.

   *The dialog **Add file entry** opens.*



Note
Files that you import into the database will be saved with the SQL database backup.
Files that you reference in the file system provide the opportunity to be replaced by other content as long as the file name does remain the same.

4. Under **Destination file** modify target path and file name, as you like to save it on the client.

   The file name may differ from the one of the source file.

5. Confirm with **OK**

Source and destination are defined. The files will be transferred on the next reboot of the clients.

The files will only be reloaded after changes have been made in file configuration or in the files themselves.

6.5. Advanced file entries

The **Advanced file entries** tab allows you to set parameters that cannot be set using the graphical user interface. For example, you can set special parameters for the Citrix ICA client configuration files or the Cisco VPN configuration file.

Configuration files must have the file format `*.ini`.
Moreover, the INI file editor of Scout Enterprise places the following requirements:

- `*.ini` files contain at least one section. Every section contains zero or more keywords.The keywords contain zero or more values.
- Each section is headed by a symbolic name that is enclosed in square brackets.
- Each keyword and its value are in the same line and are separated by an equal sign (=). One keyword can have more than one value.
- If a section name is used more than once in the same file, or if a keyword is used more than once in the same section, the last occurrence has precedence.

6.5.1. Defining individual file entries

1. In Scout Enterprise, click **Options > Advanced Options**.
   Or:
   Open the context menu of the relevant OU or device and click **Advanced settings...**
2. Click the **Advanced file entries** tab.
3. Edit the following fields:

Option	Description
File	Enter full path and file name or select from the list: Citrix ICA: `/setup/ica/wfclient.ini and /setup/ica/appsrv.ini` Cisco VPN Client: `/setup/ciscovpn/sample.pcf` Terminal: `/setup/terminal.ini`
Section	Section heading without brackets
Entry	Keyword
Value	Value which shall be assigned to the keyword. Blank, separator and multiple values are allowed. Example: `valueA,valueB,valueC;comment`

4. Click **Apply**.

*The new entries are written to the *.ini file on the next reboot of the client.*

6.5.1. Changing values of individual file entries

1. In **Advances settings > Advanced file entries**, select the entry of which you want to change the value.
2. Below, in the **Value** box, replace the current value.
3. Click **Replace**.

*The new values are written to the *.ini file on the next reboot of the client.*

6.5.1. Deleting individual file entries

1. In **Advances settings > Advanced file entries**, define a new entry: Enter **File**, **Section** and **Entry** of the relevant file entry, but leave the **value** box empty.
2. Click **Add**.

The 'empty' file entry overrides previous instructions. The file entry is deleted from the relevant section on the next reboot.

Note
If you use the **Delete** button to delete a selected row from the list, this only means that Scout Enterprise does not update the relevant entry anymore.

6.5.1. Deleting complete sections

1. In **Advances settings > Advanced file entries**, define a new entry: Enter **File** and **Section** of the relevant file entry, but leave the **Entry** and **Value** boxes empty.
2. Click **Add**.

The 'empty' section overrides previous instructions. The section is deleted from the file on the next reboot even if it contained file entries.

6.6. Rules

With the aid of this register you can define rules which can be executed when closing the last application or during the first contact with Scout Enterprise.

1. Click at the register **Rules**.
2. Define the action which should be executed during closing the last application.
3. Enter a time period in seconds for informing the user.
4. Define the action which should be executed in the case of the first contact with Scout Enterprise.
5. Confirm with**OK**.

7. Defining applications

Definition of applications and the applications themselves come up independently of each other.

Defining applications means to configure the applications provided for the user. The applications can only be used if the relevant application packages are installed on the client via IDF configuration, see Creating an IDF.

Applications can be

- Applications for backend connection
- Local Applications

Applications can be inherited from up to down. The lowest level where to define an application is an OU.

7.1. General

7.1.1. Adding applications

1. Right-click on the **Applications** icon of the relevant OU.
2. On the context menu, click **Add**.

*The **Application Properties** Dialog opens. This dialog provides several tabs, each of them relating to a particular application type.*

The following settings of the **Application Properties** are available for all application types:

Option	Description
Application restart	The application will immediately be restarted after closing.
Starting automatically after...	The application starts automatically after the eLux desktop interface has been loaded. You can delay the auto-start process when entering a particular figure (in seconds).
Desktop icon	You can define a particular desktop icon for every application (except for PN-Agent)

7.1.1. Editing application properties

- Open the context menu of the relevant application and click **Properties**.

*The **Application Properties** dialog for the application opens.*

Note
Properties of the selected application can be displayed in the **Properties** Windows of the Scout Console. They can't be modified here.

Application properties like the following ones can be seen:

Option	Description
ID	Identifier of the application
Name	Name of the application
Type	Type of application (for example **RDP**, **ICA**, **local**)
Auto-start	Application starts automatically 1 Auto-start active 0 Auto-start inactive
Hidden	Application is hidden. (only available for **local** applications of the type **user defined**) 1 Application hidden 0 Application shown normally
Kiosk	1 kiosk mode active for application type browser 0 no kiosk mode
Server	Name of the server to which the application connects
Application	Name of the application to which the application connects
User	Name of the user who is logging in
Homepage	front page for application type **Browser**
Start website	opening website for application type **Browser**
Proxy	Proxy for application type **Browser**
Free Parameters	Individual parameters for starting applications

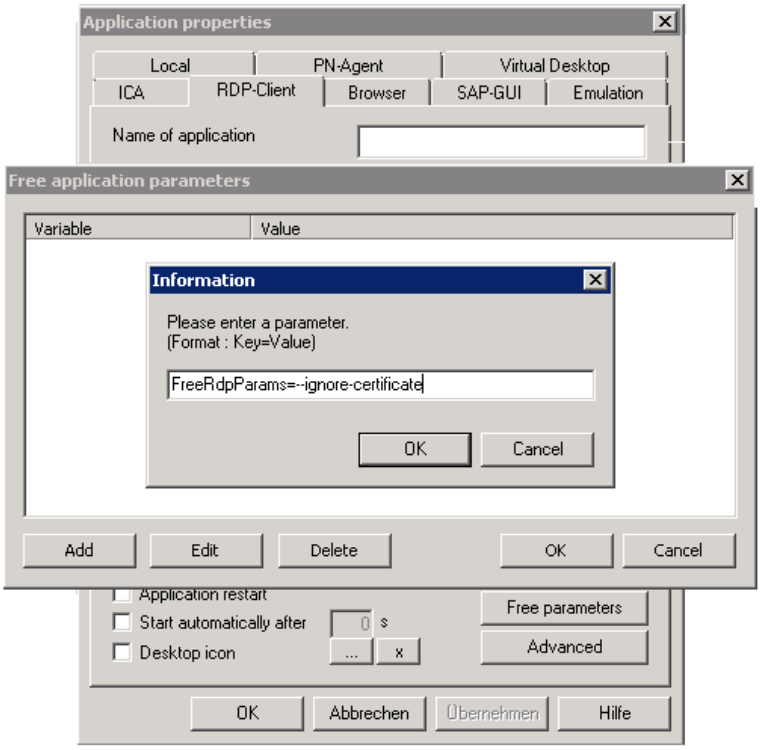
Note
Applications are identified by their name. Make sure to use a unique name for them.

7.1.1. Using Free Application Parameters

You can define individual parameters for starting any application, except SAP-GUI and Emulation.

1. Open the **Application properties** of the relevant application.
2. Click **Free Parameters**.
3. Click **Add** and enter the parameter desired using the specified format.
4. Confirm with **OK**.

The defined parameters will be inserted into the file `\setup\sessions.ini` *of the relevant applications.*



7.1.1. Using parent applications

1. Open the **Applications** context menu of any level.
2. Check the **Use parent applications** option.
3. If you want the default settings of the parent applications to be applied, check the **Use parent defaults** option.

After restarting the client interface, the applications of the parent OUs will be added to all devices of the selected level- in addition to the already existing applications.

Note
All applications and their origins are displayed in the **Device/Application list** window. Applications at root level get the value `Enterprise` in the **Origin** field.

7.1.1. Software-Defaults

Software settings for a particular application type can be defined centrally or for every OU. We recommend to apply the default settings at the top level of the applications to use inheritance for all OUs.

Note
If you want to use different default settings for different OUs, you have to disable inheritance . For more information, see Blocking inheritance

So far there are only software defaults for ICA software available. You can modify them as follows:

1. Open the **Applications** context menu.
2. Click **Edit**.
3. Modify the default settings.
4. Confirm with **OK**.

7.1.1. Uploading applications from thin client to Scout Enterprise

Important
If you upload applications to an OU, all existing applications in this OU will be deleted.

Uploading from any client

1. In Scout Enterprise, click **File > Application Upload...**.

   *The **Application upload** dialog opens.*

2. Enter the IP address or name of the client device you wish to upload applications from.
3. Select the **Destination** OU, into which the applications should be uploaded.
4. Click **Start**.

The applications of the specified thin client will be uploaded to the specified OU. Already existing applications will be deleted.

Uploading from clients managed by Scout Enterprise

1. In Scout Enterprise, select the particular device from which you like to upload the applications.
2. Click **File > Application Upload...**.

   *The **Application upload** dialog is opened. The IP-address of the selected device is already set in the field **IP-name or IP-address of the device**.*

3. Select the **Destination** OU into which the applications should be uploaded.
4. Click **Start**.

The applications of the specified thin client will be uploaded to the specified OU. Already existing applications will be deleted.

7.1.1. Defining application icons

You can define custom icons for applications that will be displayed on the client. The file types XPN, ICO and GIF are supported.

1. Open the context menu of the root level **Applications**.
2. Click **Define application icons...**.
3. Click **Add** and select the relevant file from the file system.
4. Confirm with **Open** and **OK**.

The application icon is defined in Scout Enterprise but not assigned yet.

7.1.1. Assigning an application icon

Make sure that you have defined an application icon before, see Defining Application Icons.

1. Open the context menu of a particular application and click **Properties...**.
2. Check the **Desktop icon** option.

3. Click **...** and select one of the icons.
4. Confirm with **OK** and **Apply**.

The application icon will be shown for the selected application on all clients of this OU after the next reboot.

7.1.1. Troubleshooting

Error message	Reason	Solution
Missing Firmware	The software is not installed on the thin client	Install the software on the thin client. See Management on firmware basis
doubled names	Two applications have the same name. This causes conflicts because applications are identified by their names.	Use unique names.
Hidden application can not be executed	Applications can be invisible for the user, because they run in hidden mode. This option is available for applications of the type **custom**.	Activate the option **Start automatically** or **application restart** to start hidden applications on boot or run them non-stop.
Problems with certificates in combination with VMware View Server	Server problem occurred: VMware View Server (>4.5) after successful installation is using a so-called "self-signed" certificate. If a thin client is configured correctly, it won't accept. The reason is that the **FQDN** (fully qualified domain name) is mandatory for server certificates, but is missing in the **CM**.	Create a server certificate in the **Windows-CA** with **FQDN**. Create this server certificate usingf **mmc**: Certificates (Local computer). The key must be exportable. The following steps depend on the version of the server in use: 1. From version 5.x up: The display name of the server must be **vdm**. The certificate store **local computer / personal** may contain only one certificate with exactly this name. 2. Before version 5.x in use: Export this certificate including the private key as **<name>.pfx**. Create a <password>. Save the file: C:\Programs\VmWare\VmWareView\Server\sslgateway\conf. Edit in the same directory: **locked.properties** and add the following lines: **keyfile=<name>.pfx** **keypass=<password>** Restart the VmWare View Connection server. The correct certificate will be used now.

7.2. ICA

7.2.1. General

Applications of the type **ICA**, also called **ICA sessions** or **ICA connections**, allow you to connect to a Windows terminal server with Citrix XenApp software using the Citrix ICA protocol. Thus, windows applications at terminal servers can be accessed.

For ICA applications you can define parameters on two levels:

1. Default parameters for all ICA applications can be set at Software defaults. These settings correspond to the **Settings** in Citrix ICA Receiver.
2. The connection parameters for single ICA applications can be set in the **Application properties**. Those parameters correspond to the **Properties** in Citrix ICA Receiver. These settings have a higher priority than software defaults.

You can set connection parameters and default parameters for each OU in Scout Enterprise or you can use use inheritance (see Software defaults).

Connecting to a Citrix XenApp Server can be done in five different ways:

- Connecting to a dedicated XenApp Server (always Desktop)
- Connecting to a published application (could also be a published desktop)
- Connecting via Web interface without browser: PN-Agent
- Connecting via Web interface with Browser
- Starting Citrix Receiver (Citrix tool for defining connections)

The ICA Connection Center can be defined as local application for managing connections as well.

7.2.2. Configuring a Windows desktop session

1. Click the **PN-Agent** tab.
2. Edit the following fields:

Option	Description
Name	Enter an appropriate name for this application
Published application	Clear the option
Server	IP address or name of the server
Application	Leave the box blank
Working directory	Leave the box blank
Logon data	Enables automatical logon on the terminal server (user, password, domain)
Passthrough-logon	The valuesof *$ELUXUSER $ELUXPASSWORD* and *$ELUXDOMAIN* will be sent directly to the client.
Kerberos authorization	The client uses the logon data of the Kerberos ticket created by the ADS authorization.
Smartcard authorization	Uses a smartcard for authorization.

3. Click **Apply** and **Close**.

7.2.3. Configuring a Windows application

1. Proceed like creating a Windows desktop session
2. Change the following data:

Option	Description
Application	Name of the Windows application including the corresponding paths. For example: `c:\Programme\Microsoft Office\Office\EXCEL.EXE`
Working directory	(optional) Working directory in the Windows application

3. Click **Apply** and **Finish**.

7.2.4. Acess via published applications

A connection to a published application lets a user access a predefined application and its associated environment. Published applications can be run in seamless mode, where the applications appear to the thin client as if they were running locally, each application running in its own resizable window.

If a published application is defined as a seamless window, the eLux task bar must be enabled in the desktop tab. Only then is it possible to maximize minimized windows again. Published applications require server-side and client-side configuration. In this section, we will discuss client-side configuration.

Via ICA application definition:

You can configure a session to access a published application via the eLux control panel.

1. Use the same approach like the configuration process of a published Windows application. However, make sure that the name of the application is the same like the name of the application which is published on the server.
2. Activate the checkbox **Published application**.

7.2.5. Access via Browser and Webinterface to published applications

Users are able to start with the aid of a local browser an application published via the Web interface of XenApp.

- To create or modify a browser session profile click **Application properties > Browser**. Edit the following fields:

Option	Description
Name	Enter a suitable name for the particular application. Exactly this name will appear in **Control panel > applications.**
Homepage	URL for calling up the Web interface homepage. Conventional formats are: http://<servername > or http://<servername>/Citrix/Nfuse
Kiosk mode	Do not enable kiosk mode.

For the remaining parameters, see Browser.

The local user starts the browser on the **Applications** tab of the eLux control panel and is shown the web interface site. After having logged on a list of the available and published applications will be displayed. The user then clicks an icon to start the related application.

7.2.6. Citrix Receiver

Citrix Receiver is a Citrix created tool for defining connections. Citrix Receiver can be saved locally. There are two different ways to start Citrix Receiver:

- as local application
- directly from eLux

Starting Citrix Receiver as local application

1. Create an application of the type **Local**.
   Enter the following settings:

Option	Description
Name of application	Enter a name for the application. This name will be shown at **control panel > applications**.
Local application	Choose custom
Parameter	Enter: `wfcmgr`

2. The local user starts the Citrix Receiver application via control panel. With this, PN Agent is running and after sign in the user gets a list of available applications displayed.
   To start the application click at the icon.

Starting Citrix Receiver in eLux

1. Edit an existing ICA application or choose **Setup > Configuration > New > ICA**.
2. Enter a name for the application.
3. Click at **Advanced**.
   Citrix Receiver will open.

7.2.7. ICA software defaults

The ICA software defaults correspond to the client's **Advanced** options of the ICA Client Application properties.

Any changes to the ICA default parameters defined in Scout Enterprise will affect all devices of the relevant OU.

Some of the Citrix ICA parameters are described below. For more information, see Citrix documentation.

Opening ICA software defaults

1. Open the **Applications** context menu in the tree view and click **Software defaults...**.

> **Note**
> If inheritance is enabled, you can only open and modify the **Software defaults...** of the superior (inheriting) instance, see Software defaults for applications.

2. Select **Citrix ICA-Settings**.
3. Click **Edit**.

4. Edit the desired settings of the relevant tabs and confirm with **OK**.

General tab

Option	Description
TW2StopwatchMinimum	(Default = 25) Definition of the scrolling speed of ICA applications (such as Adobe® Acrobat® Reader, Excel®, etc.). The higher the value, the slower the speed when scrolling. Note for Excel: A low value does increase scrolling speed, but speed is delayed as soon as a selection is drawn down out of the visible screen area.
Client name template	Client name in XenApp session. Note: You can use teh Program Neighborhood Variables `$ICANAME`, `$ICADOMAIN` to set a unique client session name! This is required for Citrix Roaming and some XenApp programs, for information, see Program Neighborhood Variables.

Drive Mapping tab

Assign the local resources to drive letters that you want to be shown in the ICA session. The letters A to Z represent the logic drive names of the terminal server. In the field on the right enter the mount points corresponding to the local access path of the resources such as `/media/usbdisk` or `/media/cdrom`.

For more information, see Mount points.

The attributes indicate the type of access permission:

- E = enable
- R = read
- W = write

The option **Enable Drive Mapping** must be ticked to enable the feature. The defined drive mappings are carried out only , if the option is active.

The option **Enable Dynamic Mapping** results in assignment of any available mass storage devices to the next free drive letter.

7.2.1. ICA Connection Center

By means of the ICA Connection Center the user is able to see online all current server connections of published applications He can disconnect or log off without operating the application.

The ICA Connection Center can be defined as a **local application**.

- Choose in the tab**Local** the application type **ICA Connection Center**.

7.2.2. Installing Lumension package

1. Download the package "Lumension Endpoint Security Agent Control" from the technical portal www.myelux.com > Software Packages. Make sure that you download the package for the

corresponding eLux version.

2. With the aid of ELIAS you are able to add this package into the corresponding container.
3. Add this package into your IDF and save this new IDF.
4. Execute an eLux update onto new IDF.
5. Change to the particular server on which the Lumension software is running on the server-side.
6. Finish the service **Lumension Endpoint Security Command and Control**.
7. Copy the file `LDI64.dll` into the folder `Program Files\Lumension\Endpoint`.
8. Start the service **Lumension Endpoint Security Command and Control** again.
   The log-file will belocated at **%windir%\Temp\ldi.log**.
   Further information can be found on the website of Lumension Security Inc.

7.2.3. Installing HDX Runtime-Engine

HDX runtime engine enables better audio and video quality at VOIP and video chat.

1. Download the package "HDX Runtime-Engine".
2. Add the package to a container using ELIAS.
3. Add the package to your IDF and save the IDF file.
4. Update eLux using the new IDF.
5. Configure Microsoft Lync via Microsoft Lync Server.

7.3. StoreFront

Citrix StoreFront authenticates users to XenDesktop, XenApp and VDI-in-a-Box. Available desktops and applications are aggregated and provided in stores that users access through Receiver.

StoreFront being integrated into the Modern User Interface of eLux RP enables the users to access either Citrix resources of one or more stores and any configured applications such as **RDP** or **Browser** sessions by using only one interface, the Modern User Interface.

Requirements for accessing the stores using the Modern User Interface:

- eLux RP 4.8.0 or later
- ICA client V13.1.3 or later
- In **Setup> Desktop > Advanced**, the option **Klassischer Desktop** must be disabled.

Alternatively, Citrix StoreFront can be used through the SelfService User Interface of Citrix, however, access is limited to Citrix resources.

Requirements for accessing the stores using the Citrix SelfService User Interface:

- The feature package**Self-service** component of eLux package ICA client V13.1.3 or later must be activated.
- Definition of a local application of type `Custom` and with parameter `selfservice`.

7.3.1. Configuring StoreFront

1. In the **Application properties** dialog, click the **RDP** tab.
2. Edit the following fields:

Option	Description
Name	Name for the StoreFront session
Stores	Enter the URL of one or more stores • Click **Add** and replace the auotmatically created default value by your individual values (double-click or F2) Note, that with Citrix Receiver for Linux V13 you must type in the extension `/discovery` after the URL (`https://storeURL/discovery`).

3. If you want to delete an entry from the stores list, select the entry and click **Delete**.
4. If you want to configure further settings, click **Advanced**. For more information, see Advanced StoreFront settings.
5. Confirm with **Apply** and **OK**.

Note
Using Citrix StoreFront requires the relevant certificates that must be transferred to the client. For more information on configuring file transfer, see Advanced setup/Files.

7.3.1. Advanced StoreFront settings

Option	Description
Windows properties	Choose **Full screen** or **Windowed**.
Application reconnection	Choose from • **Do not reconnect** • **Active and disconnected sessions** • **Disconnected sessions only**
Manual logoff	Choose from • **Logoff only server** • **Logoff server and applications** • **Logoff server and disconnected sessions**

7.3.2. Customizing Modern User Interface

The Modern User Interface layout can be customized to your needs. For examole, you can change the size of the application icons or dispay your own logo on the desktop. The Modern UI parameters are defined in the client file `/setup/terminal.ini` in the section [`Layout`]. To set or modify entries, use the Scout Enterprise feature Advanced file entries.

1. In Scout Enterprise console, select **Options > Advanced Setup**.
   Or:
   For the relevant OU or device, open the context menu and select **Advanced settings...**
2. Select the **Advanced file entries** tab.
3. From the **File** drop-down list on the left, select `terminal.ini`.
4. In the **Section** text box, type `Layout`.
5. Edit the text boxes **Entry** and **Value** as follows:

Eintrag	Wer-tebereich	Default	Beschreibung
DesktopLayout	small, medium, large	medium	size of the application icons on the desktop
DesktopLogo	*Path and name of the picture file*	*eLux-Logo*	Replaces the eLux Logo in the upper left by the specified picture file. Example: `setup/public/myPic.png`
	Note The picture file must be configured for file transfer. For more information, see Advanced Setup/Files		
DesktopTextColor	#<*rgb*>	#ffffff	Text colour of application icons
DesktopBack-groundColorMenu	#<*rgb*>	#000000	Background colour of menus

6. Confirm each entry with **Add**.
   For more information, see Advanced file entries.
7. If you want to display a background image in the Modern User Interface, configure the relevant picture file in device setup **Desktop > Advanced > Background**. For more information, see Advanced desktop settings.

7.4. RDP

This connection type corresponds to the ICA functionality but is using Microsoft Remote Desktop Protocol (RDP) to connect to a Microsoft Terminal Server. The free software implementations **rdesktop** and the later **FreeRDP** can be used, for both of them we provide a client. For more information, see www.rdesktop.org or www.freerdp.com, respectively.

There are two ways for configuration:

- Windows Desktop: The user accesses the desktop of a terminal server using a remote desktop session. He can use any application available on the desktop.
- Individual / seamless application: The user can only access one particular application of the terminal server.

7.4.1. Configuring remote Windows desktop session

1. In the **Application properties** dialog, click the **RDP** tab.
2. Edit the following fields:

Option	Description
Name	Name for the RDP session
Server	IP address or name of the server
Application	Leave the field blank
Working directory	Leave the field blank
Login data	Enables automatic log on to the terminal server (User, password, domain)
Passthrough login	The values `$ELUXUSER`, `$ELUXPASSWORD` and `$ELUXDOMAIN` will be sent to the client.

3. Click **Apply** and **Close**.

7.4.1. Configuring RDP application

To configure an individual RPD application you have to add the desired application to the Windows desktop definition.

1. In the **Application properties** dialog, click the **RDP** tab.
2. Edit the following fields:

Option	Description
Name	Name for the RDP session
Server	IP address or name of the server
Application	Name of the Windows application including path name. System variables are allowed. Example: `c:\Program Files\Microsoft Office\Office\EXCEL.EXE` `%SystemRoot%\system32\notepad.exe`
Working directory	(optional) Working directory of the Windows application

Option	Description
Login data	Enables automatic login to the terminal server (User, password, domain)
Passthrough login	The values `$ELUXUSER`, `$ELUXPASSWORD` and `$ELUXDOMAIN` will be sent to the client.

3. Click **Apply** and **Close**.

The user will have only one window: His application runs full-screen in the session window.

7.4.1. Advanced RDP settings

1. In the **Application properties** dialog of a RDP application click the **Advanced** button.
2. Edit the desired settings of the relevant tabs.
3. Confirm with **OK**.

View tab

In the **View** tab you can modify the window size (full screen or a specific resolution).You can define full screen on one or all monitors for multi-monitor mode and you can configure color depth (8-32 Bit).

Local Ressources tab

The **Local Ressources** tab provides additional settings for terminal servers supporting RDP protocol version V5.2 or later.

Note
The **Local Ressources** tab is only visible if the RDP client V1.3.1 or higher is installed, or if FreeRDP 1.x is installed. The settings take effect only if on the **Advanced** tab the value of the **Protocol** field is not set to `RDP V4`.

Option	Description
Drives	Select drive, mount point and drive letter that you want to be shown in the RDP session. The mount points correspond to the local access paths of the resources and are provided by eLux. For USB devices the mount points are `/media/usbdisk`, `/media/usbdisk0` and so on. For more information, see Mount points.

Option	Description
Printer	Up to four printer definitions can be created automatically for a session. The printers must be configured on the Printer tab in the eLux control panel and they must have the correct driver name as defined on the server (case-sensitive!). The first four profiles can be used with drivers. To define a default printer, enable the option **Standard** in the **eLux Printer** settings.
Sound	Using the **Play local** option, the sound can be reproduced locally on the client. **Play remote** provokes the sound to be played remotely on the server.
Connections	Turns the defined connections accessible in the RDP session.
Card reader	Smart cards based on a certificate can be used for log in.

Advanced tab

Option	Description
Protocol	Enables setting to protocol 4 or 5. Normally the protocol is recognized automatically.
Keyboard language	Defines the keyboard layout within a RDP session. The default is **Auto** which corresponds to the keyboard setting of the eLux control panel.
	Important If you define a particular language, it has to be identical with the keyboard language defined in the eLux control panel.
Deactivate Window-Manager Decorations	The frames of the eLux windows won't be shown.
Deactivate encrypting	The r server does not accept encrypted sessions. You can use this option to increase performance. By default the option is disabled.
Deactivate mouse movements	If you enable this option, mouse position data will not be transferred to the server constantly, but only with every mouse click. This increases system performance and is especially helpful for connections with small bandwidth. By default the option is disabled.
Show connection list on full screen	Shows connection list in full screen mode.
Bandwidth	Choose from `standard`, `modem`, `broadband` or `LAN`.

7.4.1. Configuring RemoteFX

Microsoft® RemoteFX™ is a new feature that is included in Windows Server 2008 R2 with Service Pack 1 (SP1). RemoteFX delivers a rich user experience for Virtual Desktop Infrastructure (VDI) by providing a virtual 3D adapter, intelligent codecs and the ability to redirect USB devices to virtual machines.

1. Right click on device **rdp connection > Properties > Advanced**.
2. Choose **Advanced**.
3. Set bandwidth to **<LAN>**.
4. Reboot the thin client.
   The bandwidth option of the rdp connection defined gets activated.

Note

RemoteFX will only work if the server supports RemoteFX and is configured in the right way. There is no possibility to setup RemoteFX specific parameters on the thin client. All parameters will be provided by the server.

7.5. Browser

Mozilla Firefox is used as browser. For more information about Firefox see www.mozilla.org.

7.5.1. Configuring browser session

1. In the **Application properties** dialog, click the **Browser** tab.
2. Edit the following fields:

Option	Description
Name	Enter a name for the browser such as `Firefox`
Home Page	Website that opens whenever you click **Home**
Start Page	Website that opens after starting the browser
Proxy type	`No proxy`:No proxy server used `Manual (Proxy:Port)`:Enter proxy server and port number using the format `<Proxy server name or IP address>:<port number>` `Auto (URL)`:Proxy configuration file (*.pac). Example: `http://www.domain.com/autoproxy.pac`
Browser type	If there have been installed several browsers, you can select one of them.

3. Confirm with **Apply** and **Close**.

Note
By default, all browser files (cache, history, bookmarks, etc.) are saved temporarily to the device flash memory. Since capacity is limited, we recommend to configure the browser home directory on a network drive. For more information, see Browser home directory.

Note
Providing certificates for the browser has to be done by transferring them to the local directory `/setup/cacerts/firefox` of the client. For file transfer use the **Files** feature, see Files.

Note that a second boot of the client is required to assign the certificates that have been transferred during the first boot to the certificate store of the browser.

7.5.1. Configuring Kiosk mode

Kiosk starts the browser in fullscreen mode and with limited user rights. The user cannot open any tabs and cannot exit the browser. Kiosk mode is suited if the user should only see one website and if he is not supposed to use further applications on the thin client. For good use of this function, we recommend to disable related functions of the thin clientsuch as rebooting and opening the control panel. For more information, see Setup>Security.

1. Click **Advanced**.
2. Check the **Kiosk** option.

3. Select the **Navigation bar**, **Address bar** and **Print button** options, if you want to show them to the user.

   This functionality works only with Firefox 3.6x.

4. Confirm with **OK** and **Apply**.

The next time you start the browser it will open in Kiosk mode.

7.6. Local

Defining local commands is particularly important as they enable defining applications which can be called within a shell. This feature assumes knowledge about the commands that the average user may not have.

Make sure that the user is authorized to start particular applications. All commands are carried out by the UNIX user**eLux** (UID = 65534).

Error messages will not be shown. If the entered command does not show a x-capable application during execution process you also won't see anything concerning a possible error.

For this reason we recommend you to execute the command first of all within a x Term session for testing purposes and for preventing possible errors.

7.6.1. Configuring local applications

1. In the **Application Properties** dialog, click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Enter an appropriate name for your application.
Application	Application type
	Note Some local application types are predefined. If the desired application does not exist in the list, click `Custom`. Note that in this case you have to enter the program start up command in the **Parameter** box.
Parameter	(optional) Enter program start up parameters. For custom applications enter the complete command. Example: `squid` calls the custom application **Squid**. `squid /tmp/mycache` calls Squid using a particlar cache directory.
Hidden (only for application type `Custom`)	Application will not be displayed on the **Application** tab. The option **Start automatically** or **Application restart** must be active.

3. Click **Apply** and **OK**.

7.7. PN-Agent

7.7.1. General

The Program Neighborhood Agent enables users to connect to published resources (i.e. published applications and published content) through a server running the Web Interface.The configuration for all users is defined in the configuration file config.xml, which is stored on your server running the Web Interface. The default location for config.xml on a server is: //Inetpub/wwwroot/Citrix/PNAgent.

The PN-Agent downloads its configuration data from the server running the Web Interface when it is started, and can be configured to update settings and the user interface regularly.

The file config.xml should only be edited with the aid of the PN agent management tool. Detailed information regarding the editing of the config.xml via a web interface can be found in the Citrix edocs .

7.7.2. Advanced PN Agent settings

1. Click the **Advanced** button.
2. Edit the following fields:

Option	Description
window properties	Adapt here the resolution, color depths as well as the audio output. Standard applies the settings of the server.
Timed logoff	You can schedule logging off from a PN Agent session by a period of time predefined (in seconds), allowing not to await the last PN Agent application to close.
Manual logoff	Choose from three options for manually logging off: • Log off only the server • Log off server and applications • Log off server and disconnect applications
Application reconnection	Choose from three options for using an automatic connection buildup: • Do not reconnect (default) • Active and disconnected sessions • Disconnected sessions only

3. Click **OK**.

7.7.3. Configuring PN-Agent manually on the thin client

1. Select the **PN-Agent** tab.
2. Edit the following fields:

Option	Description
Name	Enter an appropriate name

Option	Description
Server	Enter the IP address or the name of the server. Alternatively, if the Citrix Web interface is not running on port 80 or if the configuration file does not have the standard path `/Citrix/PNAgent/config.xml`, you can enter an URL to direct the client to the configuration file on the server. Format: http://<server>:<port> or http://<server>/<path> . For example: `http://server-1/Citrix/PNAgent/config.xml` `http://server1:81` `http://server1/MyNfuse/config.xml`
Logon	Enables automatic logon to the terminal server (user, password, domain).
Passthrough-logon	The following values will be sent to the client: `<$ELUXUSER>` `<$ELUXPASSWORD>` and `<$ELUXDOMAIN>`
Kerberos-authorization	The client uses the logon data which was received during ADS authorization of the Kerberos ticket.
Autostart-folder	On the server, in Program Neighborhood Agent create a folder (or subfolder) with published applications. Enter the name of the folder here. All published applications in this folder will automatically be started when the session connects.
Show last user	The user credentials (except for password) of the last logon will automatically be displayed in the XenApp logon dialog box. Note that this option has no effect if you enter user credentials for automatic logon.
Allow cancel	Allows the user to close the XenApp logon dialog box.

3. Click **Apply** and **Finish**.

7.7.4. Program Neighborhood Variables

For example ,variables can be used to define a unique client name for a Citrix XenApp session. For logon to XenApp web server with Program Neighborhood you can use the following variables:

$ICAUSER	User name
$ICADOMAIN	Domain for this user
$ICAAPPLICATION	Name of the PN-Agent application definition

7.7.5. Creating a domain list

For selection purposes of the end user you are able to create a domain list for PN Agent and XEN Desktop.

1. Create the text file **icadomains**.
2. Enter the domain name desired (one domain per line).
3. Save the file in the Scout Enterprise installation directory.
4. Transfer the file into the directory **Setup** which is located on the thin client. Transfer with the aid of the Scout Enterprise file transfer function. In the case that not all information was provided during

configuration when starting the PN Agent or the XEN Desktop application a dialog opens for registration on the Citrix XenApp webserver. The domains will be offered as drop-down list. Additionally you are able to preset in the PN Agent application definitions a domain. For example **work.myelux.com**.

7.8. Emulation

7.8.1. Available Emulations

Emulation	Description
X32, X52	3270/5250 Emulation is a licensed product from Unicon Software GmbH. 3270 and 5250 come together as the package Terminal emulation for Motif(xemu). It includes a 15-minute trial period. The software is available via Unicon software and partners. You can find the latest user manual in the Archive. Emulation X97 by Unicon Software was available for eLux NG, but is no longer available for eLux RL and RP.
eterm	eterm is a terminal emulation suite that includes the following emulations: Siemens 97801 (7 & 8 bit), ANSI, AT386, BA-80, VT320 To use this software, you have to have the "Eterm 97801 terminal emulation (eterm) package" installed. eterm is included in licensed eLux software free of charge. For configuration information or how to modify the key mapping, see the eterm Administrator's Guide, available at the Archive.
Tarantella	Tarantella allows users to access their applications over a Web-based interface. To use this software, you must have the Terminal emulation for Motif(xemu) package installed. The server is licensed, the client is free. For more information, see www.tarantella.com.
Virtual Network Computing	Virtual Network Computing (VNC) is a remote display system which allows you to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. The remote machine to be viewed must have a VNC server installed and the local machine a VNC viewer. The option in the Emulations dialog is for configuring the VNC viewer, which is open source and included free with eLux software. To use this software, you have to have the VNC client (vnc) package of the eLux package "Mirror eLux Desktop" installed.Further information concerning VNC can be found at the chapter Mirroring.
XDMCP	The X Display Manager Control Protocol (XDMCP) is used by X terminals (and X servers in general) to set up an X session with a remote system over the network. The XDMCP functionality is included in the base OS. By default, the XDMCP session runs in its own console. To enable sound, open **Setup > Multimedia** and check the **Enable sound in XDMCP sessions** option. Note: The application must be e-sound system compatible.
X11	The X Window System (X11) is the de facto standard graphical engine for the UNIX and Linux operating systems. It provides common windowing environment bridging heterogeneous platforms. It is independent of operating system and hardware. The X11 server developed by The XFree86 Project, Inc (www.xfree86.org) is included in the Xorg XWindows package.
PowerTerm InterConnect	PowerTerm® InterConnect from Ericom® Software is an emulation suite that allows you to connect to IBM mainframes, IBM AS/400, Unix, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000 and Data General. Using this software requires the installation of PowerTerm InterConnect (powerterm) package. PowerTerm InterConnect is a licensed product, to acquire a license please contact Unicon Software or one of our distribution partners.

7.8.2. Configuring X11

1. Add a new application and click the **Emulation** tab.
2. In the **Emulation type** list, click **X11**.
3. Edit the following fields:

Option	Description
Name of application	Enter an appropriate name for this application, such as `X11`. Do not use blanks in the name.
Server address	Enter the IP address or the IP name of the UNIX server.
User name	Enter the name of the user registered on the UNIX system.
Application	Enter the application name including its complete path.
Use SSH	The X11 session is started via the Secure Shell (SSH) protocol. Only public key authorization is possible.

4. Confirm with **Apply**.

7.8.1. Configuring PowerTerm

Configuration of PowerTerm InterConnect is carried out in two steps:

- Configuring the PowerTerm application on a reference client and transferring the created configuration files
- Configuring the PowerTerm application for all clients using the configuration files created on the reference client

Configuring PowerTerm InterConnect for reference client

The PowerTerm software package must be installed on the reference client

1. Define on the reference client locally or in Scout Enterprise console a PowerTerm application containing only the application name. (for details see below).
2. Start PowerTerm on the reference client and configure the application manually.

   The configuration will be saved in the local client directory `/setup/PowerTerm/` *in the following four files*

   `ptdef.pts`
   `ptdef.ptc`
   `ptdef.ptk`
   `ptdef.ptp`
3. Close PowerTerm.
4. Copy the four configuration files via network or USB flash drive and make them available to Scout Enterprise console.
   Or:
   Transmit the files from the client to Scout Enterprise console remotely by using **Request diagnostic files** with an individual template. For more information, see Modifying device diagnostics.

The configuration files for the actual PowerTerm configuration are provided. The second step may be carried out.

Configuring PowerTerm InterConnect for all clients

1. In Scout Enterprise console add a new application for the desired OU.
2. On the **Emulation** tab, in the **Emulation type** list, click `PowerTerm`.
3. Edit the following fields:

Option	Description
Name of application	Enter an appropriate name without using blanks.

Option	Description
Parameters	Optional starting parameters for the PowerTerm application: `-fullscreen` full screen `-maximize` maximized window `-no-menu-bar` no menu bar `-no-tool-bar` no toolbar `[myName].pts` name of an individual PowerTerm configuration file of the client Example 1: `-fullscreen -no-menu-bar -no-tool-bar` Example 2: `-fullscreen ptconfig001.pts`
Terminal setup file	Select the relevant `.pts` file of the reference client from the file system.
Communication file	Select the relevant `.ptc` file of the reference client from the file system.
Keyboard file	Select the relevant `.ptk` file of the reference client from the file system.
Power PAD file	Select the relevant `.ptp` file of the reference client from the file system.
x button	Delete previously selected configuration file from the Scout Enterprise database if required. To delete the file physically from the client you need to perform a factory reset.

4. Confirm with **Apply**.

PowerTerm InterConnect will be available to all clients of the relevant OU on the next boot.

7.9. SAP GUI

Using the feature **SAP GUI** the software **SAP R/3 client PlatinGUI** (**sapplatingui**) and **IBMJAVA2** has to be installed.

eLux supports the SAP/R3 client from eLux RL2.10 on. However, this feature is not available for all hardware platforms. Please check in the relevant eLux container on www.myelux.com whether SAP R/3 client is available.

Minimum system requirements:

1. 96 MB free hard drive space
2. 128 MB RAM

7.9.1. Configuring SAP GUI

1. In the **Application properties** dialog, click the **SAP GUI** tab.
2. Enter a name for the application.
3. Check the **Classical user interface** option , if you like to use the classic SAP design.
4. Confirm with **OK**.

There are two ways to configure the SAP client:

Local on the client	SAP GUI can be configured directly on the thin client when the user starts the SAP client for the first time.
Configuration via administrator	The administrator can transfer a SAP configuration file or message server list to the relevant devices. The SAP client configuration file is `/setup/sapgui/platin.ini`. For more information about how to transfer files see Transferring Files.

Note
For more information on SAP GUI configuration, see SAP documentation.

8. Online commands

8.1. Scheduling and executing commands

With the aid of Scout Enterprise the administrator is able to change the status of the devices. Those commands can be executed immediately or at a defined point in time.

1. Choose **Right click on device > commands**.
   Choose from the following commands:

Command	Description
Switch on	Switches on the device.
Switch off	Switches off the device.
Restart desktop	Restarts the interface.
Restart device	Reboots a device.
Send message	Sends a message to the device. Text can be formatted with the aid of HTML-tags.
Update	Executes a firmware update.
Refresh device status	Calls for the current device status of a particular device.
Remote factory reset	Sets the particular device back to its initial state. Both the Scout Enterprise Server address and the licenses are remaining on the client. Options: - Delete Scout Enterprise Server address on the client (analogue initial state on the client) - Delete saved licenses on the client (for example due to resale)

2. Choose from the list the particular command you like to execute.
   The window **Executing command/scheduling** opens.
3. Choose whether the user is to be informed and is able to cancel the particular command.
4. Choose at which point in time the command should be executed and whether it should be executed again or not.

8.2. Mirroring

8.2.1. General

Basically, mirroring serves the purpose that one person can display or 'mirror' the client desktop of another person in the same network. On the mirrored computer, even mouse and keyboard control for the mirrored computer can be given to the remote person. This enables use cases where the administrator does not have to be present physically but can provide help remotely - e.g. for administration or support purposes.

Mirroring the screen of a client creates several advantages for both the end-user and the system administrator. An administrator can check directly on a client for example if a new software application is working properly. Moreover, even during the user's active workday an administrator or a supporter can look at end-users' problems and provide a solution while both are looking at the same mirrored desktop.

8.2.2. Requirements

On the administration system, you only need one of these three options (but you can also use all three of them):

- Install Scout Enterprise which has the mirror capability built-in (from the Scout Enterprise console you can mirror clients).
- Install the Scout Enterprise Mirror Tool.
- Install a VNC viewer.

On the target device:

- Install a VNC server. For eLux clients: install the "mirror" package.

8.2.3. Mirroring devices

It is not possible to mirror a client secretly without the user's knowledge. During the mirroring session a dialog appears both on the user's and on the administrator’s screen. This dialog enables to cancel the mirroring session anytime. Additionally, a password can be defined for the mirroring session. Moreover, should you have reservations concerning the security, deactivate the mirroring settings and uninstall the mirroring software on the thin client.

This functionality is based on three steps:

1. Installing the software.
2. Configuring thin client mirroring settings.
3. Opening a mirroring session in Scout Enterprise.

Installing the software

You must have a VNC viewer installed on the administrator’s machine, and a mirroring server on the target device. A VNC viewer is included in the Scout Enterprise Server software. No further action is required. A mirroring server must be installed on the thin client.

For Thin Clients with the operating system eLux the mirroring server will be installed with the 'mirror' package. Add the mirror package to the Thin Client's IDF file and update the client. After the update, the mirror package will be part of the installed image.

Configuring thin client mirroring settings

As soon as the mirroring package is installed, you have to allow the mirroring session directly on the thin client. Also you have to define a password. Find further information concerning mirroring settings in security.

Opening a mirroring session in Scout Enterprise

Note

Only a single device can be mirrored. If there are two monitors connected on one client, both monitors are mirrored. To get the best result, make sure to have connected two monitors also on the Scout Enterprise machine, set to the same screen resolution as the two client monitors. During mirroring session the keyboard layout is used as defined on the Scout Enterprise machine. The keyboard layout of the client is not used.

1. Choose right click on **Devices > Mirroring.**
2. Choose the type of connection:

Option	Description
Desktop	Mirroring the eLux desktop (Display 0).
XDMCP 1	Mirroring the first opened XDMCP session (Display 1).
XDMCP 2	Mirroring the second opened XDMCP (Display 2).

3. Depending on the type of configuration you have to define a password.
4. Depending on the configuration the user has to confirm the mirroring session.
   The mirroring session starts.
   On the user's screen a dialog window appears during the mirroring process. This window cannot be closed.
   In the dialog window you can choose from the following options:

Option	Description
Starting connection	Defines whether another mirroring session will be possible after this session.
Confirmation requested	Defines whether a user has to confirm the next mirroring session or not.
Only demonstration	If active, no mouse and keyboard inputs executed by the administrator are transferred into the mirroring session.

5. The user or respectively the administrator finishes the mirroring session via **Finish session**.

8.2.4. Mirroring without the use of a Scout Enterprise console

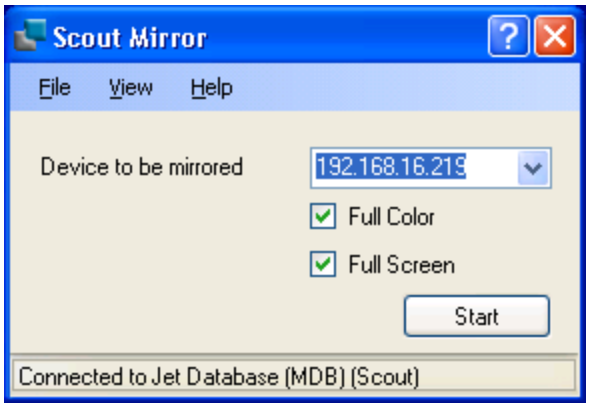
In order to avoid increased server load and to enhance the help-desk possibilities, a separate mirroring tool is available. This tool, called Scout Enterprise Mirror, can be run as a standalone program and therefore the Scout Enterprise console does not need to be started. The administrator rights defined in the Scout Enterprise console will also be applied to the mirror tool.

Requirements of the Scout Enterprise Mirror tool

1. Check the **Allow Scout Enterprise only** option in the **Advanced mirror settings**:
   In Scout Enterprise, click **Options > Base configuration > Security > Mirroring settings >**

Advanced.
Locally on the client, in the control panel, click **Setup > Security >Mirror server settings > Advanced**.

2. Turn on the object permissions **Execute mirror** and **Visible**:
   In Scout Enterprise, click **Security > Manage administrators > Default object rights**.
3. Turn on the base permission **Use of Scout Enterprise Mirror**:
   In Scout Enterprise, click **Security > Manage administrators > Edit base permissions**.
4. Download the program **Scout Enterprise Mirror Application** from www.myelux.com.



Screenshot refers to Scout Enterprise Mirror Tool V1.0.1

Note

The device to be mirrored can be accessed by entering its IP address, host name or MAC address.

8.3. Executing the setup comparison

- For the desired device open the context menu and click **Device diagnostics > Setup comparison**.
  Or:
  Select the desired device and use the hotkey STRG-E.

The configuration of the selected device will be compared to the currently stored values in Scout Enterprise database. Properties that differ will be listed in a window.

8.4. Device diagnostics

Device diagnostics helps you transfer protocol and configuration files from the client to Scout Enterprise for diagnostic purposes. The client files support error analysis and are asked in case of opening a support ticket.

You can also use this feature to request any files that you have defined.

8.4.1. Configuring diagnostic files

For device diagnosis using diagnostic files you will find a predefined template called `#System`. This template includes a file list containing relevant configuration and log files and , secondly, script code to be run on the client. Both of them can't be edited .The `#System` template is used each time device diagnosis is performed via **Request**.

In addition you can define further templates containing file lists and script.

Defining a template for device diagnosis

1. For the desired device, open the context menu and click **Device diagnostics > Request files**.

   *The dialog Edit diagnostic files opens. Under **Templates**, the predefined `#System` template and , if defined, further templates are shown .*

2. Click **New...**, and then enter a name for your new template.Confirm with **OK**.
3. In the **Templates** list, click your new template.
4. Click **Edit** next to the file list, and then, in the text box, enter line by line the relevant file names including paths. Confirm with **Save**.
5. Click **Edit** next to **Additional script** and enter the code you want to be performed on the client. Confirm with **Save**.

Note
When performing device diagnosis with **Request** all active templates will be included.

8.4.1. Requesting diagnostic files

Note
Before performing device diagnosis you should temporarily enable enhanced debugging on the client to make sure to retrieve all data needed. After this disable debugging mode, otherwise you risk to exceed flash memory capacity of the thin client.

1. For the relevant device open the context menu and click **Setup...**.
   On the **General** tab clear the option **Use parent**.
   On the **Diagnosis** tab set the **Debug level** option to `On`.
   Confirm and perform a reboot of the client.

   Enhanced debugging on the client will be enabled.

2. For the relevant device open the context menu and click **Device diagnosis > Request files...**.

   *The **Edit diagnostic files** Dialog opens. Under **Templates** any already defined file lists are displayed, as well as the predefined `#System` template which is invariably active.*

3. If desired, check further templates of the list.
4. Click **Request**.

   All script defined in the active templates is performed on the client.
   All files defined in the active templates are retrieved from the client and saved as ZIP file in the local directory such as

   `%userprofile%\Documents\UniCon\Scout\Console\Diag`.
5. Click **Explorer**.

   The Windows Explorer opens showing the target directory.
   The latest ZIP file contains the relevant diagnostic files.
6. For the relevant device open the context menu and click **Setup...**.
   On the **Diagnosis** tab set the **Debug level** option to `Off`.
   On the **General** tab check the option **Use parent**.

   Enhanced debugging on the client will be disabled and setup inheritance will be restored.

Note
Whenever you wish to use this feature to transfer any files defined in an individual template, you do not need to carry out step 1 and 5.

8.5. Setup of OUs/Comparing devices

Comparing configuration of different OUs or devices is done by using a dedicated window.

1. Click **View> Window > Compare setups**.

   *The window **Compare setups** will be displayed as permanent window in the lower part of the console window.*

2. Drag two or more OUs or devices into the **Compare setups** window using Drag&Drop.
   Or:
   In the context menu of the relevant OU or device click **Edit > Add to setup compare...**.

3. Click the icon in the icon bar of the **Compare setups** window.

   The configurations of the listed OUs or devices will be compared. Differences in the main properties are shown.

4. If you want to view all of the information , click the icon in the icon bar of the **Compare setups** window.

   All properties are shown.

8.6. Scout Enterprise commands for WES7

The following Scout Enterprise commands work with WES7:

- Command: Update
- Command: Switch on
- Command: Switch off
- Command: Restart interface
- Command: Restart device
- Command: Remote factory reset
- Command: Send messages
- Mirror
- Device diagnostic: Request files

8.7. Switching OU to the highest level

- For the relevant OU open the context menu and click **Edit > Convert to base-OU**.

The relevant OU will be moved to the highest level.It is one of the base-OUs. Configuration and inheritance remain as defined. If inheritance is active, it will get all settings from the base configuration.

9. Firmware Update

On delivery, the thin clients are already equipped with operating system and the basic software components such as ICA client, RDP client, browser and emulations. This software called firmware is based on the flash. Whenever new software versions are available or demands are changing, software components need to be added or removed which requires a firmware update.

Firmware update includes four basic steps:

- Download of the relevant software packages from myelux.com
- Modifying the IDF on the web server using ELIAS.
- Checking the firmware configuration of the relevant thin clients
- Performing the update

Note
Firmware updates can be run automatically during boot or shutdown of the clients, but they can also be triggered by command.

Wishing to save bandwith you can use a proxy client for updates. For more information, see Update through proxy client.

9.1. Requirements

The following components are required to perform a firmware update:

- Scout Enterprise Server and Scout Enterprise console to configure firmware updating for the clients
- ELIAS tool to create and modify Image Definition files (IDF) in the software container
- Web server (HTTP, HTTPS, FTP, FTPS) with container directory providing eLux software packages and Image Definition Files
- eLux software packages to be installed

Scout Enterprise Server and console including the ELIAS tool can be downloaded from www.myelux.com. These components are part of the standard installation.

The current software bundle `eLux`*`version`*`_AllPackages.zip` and further software packages can also be downloaded from www.myelux.com.

As a webserver you can use Microsoft IIS or any other web server such as Apache.
Make sure to have enabled the relevant webserver role.

9.2. Planning and performing an update via the network

Note
The following procedure includes firmware configuration of the clients. Once configured, updates can be performed by carrying out just the first two steps, if suitably configured.

1. If the software container does not contain the relevant software, download the desired packages. For more information, see Importing packages to a container in ELIASmanual.
2. In ELIAS, modify the relevant IDF in order to provide the desired software features. For more information, see Create IDF in ELIAS manual.
3. For the relevant OU or the relevant device, open the **Setup** dialog.
   If you want to perform the update for all clients, click **Options > Base configuration**.
4. On the **Firmware** tab, check the proper configuration of firmware updating, in particular the entries of the **Protocol**, **Server**, **Path** and **Image file** fields.

   *From these values the URL below of the **Path** box is generated. The URL is relevant for the transfer of image file and eLux software packages.*

   The specified image file must match the image file updated in ELIAS.
5. If you want to have the update performed automatically on boot or shutdown of the clients, select the relevant option **Check for update** in the bottom area of the **Firmware** tab.

For more information, see Setup/Firmware.
If you want to perform updates using a proxy, see Update through proxy client.

6. Confirm with **OK**.

The firmware update is configured for the relevant clients.

*If an updated IDF is available, and if one of the **Check for update** options is selected, the update will be performed on the next reboot or shutdown, respectively.*

If you want to trigger the update using a command, add the following steps:

7. On the **Firmware** tab, click **Reminder...** to check the reminder settings for possible update deferments by the user. For more information, see Update deferment through user.
8. Confirm and then close the **Setup** dialog.
9. For the relevant OU or the relevant device, open the context menu and click **Commands > Update...**.
10. In the **Execute command** dialog, define time and more options for the update. For more information, see Scheduling and executing commands.
11. Click **Execute**.

The update process will be released at the defined time. If an updated IDF is available, the update will be performed and the client will be rebooted.

*The update status is displayed for each device in its **Properties** window. For more information, see* Update log.

9.3. Update Log

Feedback on updates is available both for a particular device in the **Properties** window and independent of the device in the **Command history** window. All update processes are recorded, even if they turn out to be obsolete and haven't been run or if they are aborted. If they have been completed successfully, they have a green symbol.

Viewing update information on a particular device

1. Make sure to show the **Properties** window: **View > Window > Properties**.

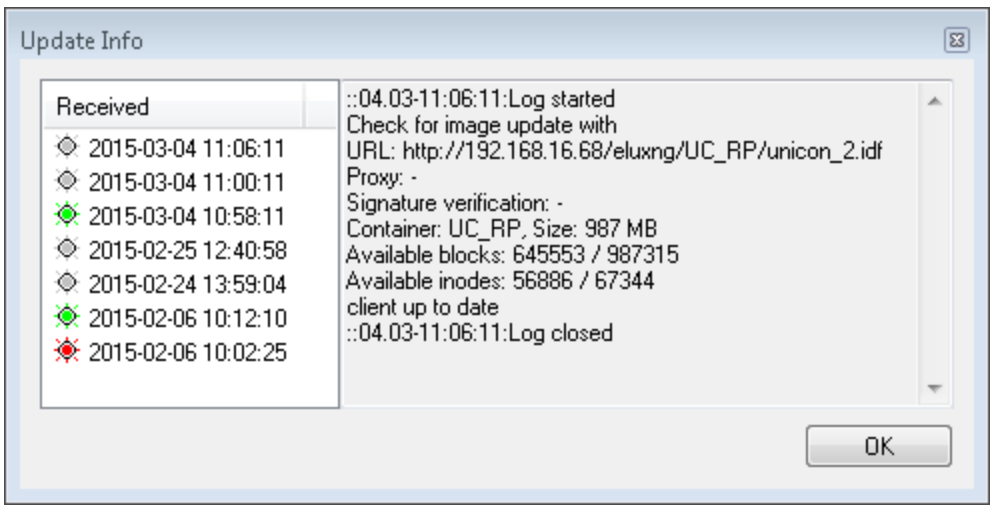
   *The **Properties** window is shown permanently in the upper right. For the selected device some properties are shown. Properties can be shown or hidden using the* *icon.*

2. Select the relevant device in the tree view.

   *In the **Properties** window, next to the **Update status** field, the current status is displayed, such as 'Update in progress', 'Update successful' or 'Update not necessary'.*

3. Double-click the term **Update status** or click **...** at the end of the line.

   *The **Update Info** window is displayed. On the left side, you can see all updates that have been processed, aborted or not been processed because the IDF had been up-to-date. For a selected update you can view all logged data on the right side, among them the installed software packages.*



Note
Information on the last update of the relevant device can also be viewed using the context menu and **Commands > Update-Info...**.

Viewing update information on all devices

Any performed updates are recorded among other performed commands independently of the device in the window **Command history**.

- Select **View > Command history...**.

*The window **Command history** opens. Scout Enterprise displays all of the performed commands and the related devices or OUs since installation of Scout Enterprise. More information on a particular process is available in the relevant **Properties** window by double-clicking the **Update status** or **Command status** field, respectively.*

9.4. Update through proxy client

If you want to update narrow-band connected clients, you might wish to use a proxy client to forward the firmware update. As proxy server software the free Squid is used.

Note
Using a thin client as a proxy requires 1 GB RAM or more main memory, since the packages are provided locally in the RAM of the proxy client. Depending on the overall size of the packages defined by the IDF you might need even more RAM.

Configuration in Scout Enterprise includes three basic steps:

- Creating an application definition for Squid
- Setting up the proxy client
- Configuring the relevant devices for the proxy update

Creating application definition for Squid

1. Create a new OU which will be configured particularly for the proxy client.
2. In this OU, define a new local application, see Adding applications.
3. On the **Local** tab, make the following settings:

Option	Value
Name of application	`Squid`
Local application	`Custom`
Parameter	`squid`
Hidden	On
Start automatically after 0 seconds	On

4. Move the proxy client into the OU and restart the client.

The client gets the Squid application definition.

Setting up the proxy client

1. Provide the proxy client with a firmware update containing the Squid software package. For this, modify the IDF using ELIAS. For more information, see Performing an update.

   After restarting, the Squid software is installed on the proxy client.

2. For the OU of the proxy client, open **Setup > General** and clear the **Use parent** option.

   Inheritance is disabled and the proxy OU can be configured independently.

3. For the OU of the proxy, select **Setup > Network > LAN**, and then select the first entry and click **Edit**.
   In the **Edit network profile** dialog, select the option **Use following IP address**.
   Leave the **Domain** box empty and confirm with **OK**.

The last obtained IP address is used as static IP address by the proxy client.

Configuring devices for the proxy update

1. For the OU or the device which you want to update through the proxy client, open the **Setup** dialog. If you want to define the proxy for all clients, select **Options > Base configuration**.
2. On the **Firmware** tab, make the following settings:

Protocol	`HTTP`
Proxy	`<IP address of proxy client>:3128`

3. Edit the further fields as usual, see Setup/Firmware.

The relevant clients get their firmware updates from the proxy client.

9.5. Troubleshooting

Error messages

Error message	Solution
Bad container	Containers are hardware-specific. Check if the container matches your thin client specifications.
Bad flash size	Verify if the flash capacity defined in the IDF matches with the actual flash capacity of the thin client.
Bad authorization	Wrong client password: Correct the entry in **Setup > Security**.
Client needs recovery information	If critical FPMs are updated in the baseOS, the thin client requires a recovery installation before it can be updated. For more information see Installing eLux RP in **eLux RP Live-Stick**-Guide.

Update options

If the update is still faulty, try to modify update settings. For more information, see Advanced setup > Update options.

10. Passwords

10.1. Local device password

10.1.1. General

The device password affects only the local device. In the local Setup of the thin client you can change the device password manually. In the initial state this password is: `elux`.

The device password is required for verifying access rights. Scout Enterprise needs the device password in for varous management actions such as updates. Therefore, it is necessary to be familiar with this password before you start for example an update process. In the case that devices are already registered in the Scout Enterprise console the access rights for this special devices are also already verified. From now on you are able to change the password for this already registered devices in Scout Enterprise.

Note

We recommend you to change the password in order to avoid unauthorized configurations caused for example by local users.

You can find further information concerning this topic in the chapter client password.

10.1.2. Changing local device password manually on the client

1. Start the eLux control panel.
2. Click **Setup > Security**.
3. Under **Local security**, click **Edit**.
4. In the **Password** box, enter a new password and repeat it in the **Password confirmation** box.
5. Confirm with **OK**.

10.1.3. Changing local device password via Scout Enterprise

With the aid of this function you can change the device password of one or of all devices managed by Scout Enterprise or of all devices of an OU.

1. If you want to change the password for all devices select **Options > Base Configuration...> Security > Local Security**.
   If you want to change the password for a particular device or OU, open the relevant context menu and click **Setup...> Security > Local Security**.

1. Click **Edit**.
2. In the **Password** box, enter a new password and repeat it in the **Password confirmation** box.
3. Confirm with **OK**.

The new device password will be assigned to all relevant and active devices. If a device is not turned on, the new password will be assigned on the nextreboot. This action affects only the devices which are registered in Scout Enterprise.

10.2. Changing Scout Enterprise console password

The server password is the password for the Scout Enterprise console. The menu command **Options > Change server password** is only active if the menu command **Security > Activate Administrator Policies...** is not checked. We recommend to enable Administrator management. Then the server password is identical to the password of your Windows account.

In the initial state the password is `elux` (all lowercase). To prevent unauthorized access it is recommended to change it immediately.

1. Log in to Scout Enterprise as administrator.
2. Click **Options > Changing server password...**

   If the menu entry is disabled, you don't have admin rights.
3. In the field **Password** enter a new password and repeat it in the field **Password confirmation**.
4. Confirm with **OK**.

11. Managing administrators

11.1. Activating administrator management

Managing several Scout Enterprise administrators requires activating the **Administrator management** feature. Scout Enterprise administrator accounts are based on Windows accounts which have to be defined before.Scout Enterprise administrator accounts can be configured in many ways.

By default administrator management is not active.

Note
Activating administrator management requires being logged in as full access administrator. The initial account is `Administrator` with password `eLux`.

1. In Scout Enterprise console, click **Security > Activate administrator policies**.
2. Confirm with **OK**.

You will be logged out and from now on you can only log in using your Windows account.
*All options of the **Security** tab as well as all options in **Options > Change Server password** will be activated.*

11.2. Adding an administrator

1. In Scout Enterprise console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, click **Add Administrators**.

   *The **Initial administrator profile** dialog opens.*
3. Select the access range for the new admin.
4. Confirm with **OK**.

   *The Windows **Permissions for Administrators** dialog opens.*
5. Click **Add...**
6. Enter the relevant user name and click **Check Names**.
   Or:
   Search for the user using the **Advanced...** button.
7. Confirm with **OK**.

The new user is added to the list of administrators. You can assign the appropriate permissions to him now. The new administrator can log on using his Windows account information.

11.3. Deleting an administrator

1. In Scout Enterprise console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Delete administrator**.

The selected administrator will be deleted without an 'are you sure?' verfication.

11.4. Administrator policy

For all Scout Enterprise administrators there are three differnet kinds of permissions:

Base permissions	Main access permissions (total control)
Menu permissions	Access permissions for specific menu commands
Object permissions	Access permissions for Organization units, groups and/or individual devices

In the relevant **Administrator rights** dialog the provided rights are displayed with a green or red symbol:

Access granted	
Access denied	

By using double-click or pressing the space key, the rights can be turned on and off.

If you use the buttons **Full access** or **No access**, all of the displayed rights will be set to green or red, respectively.

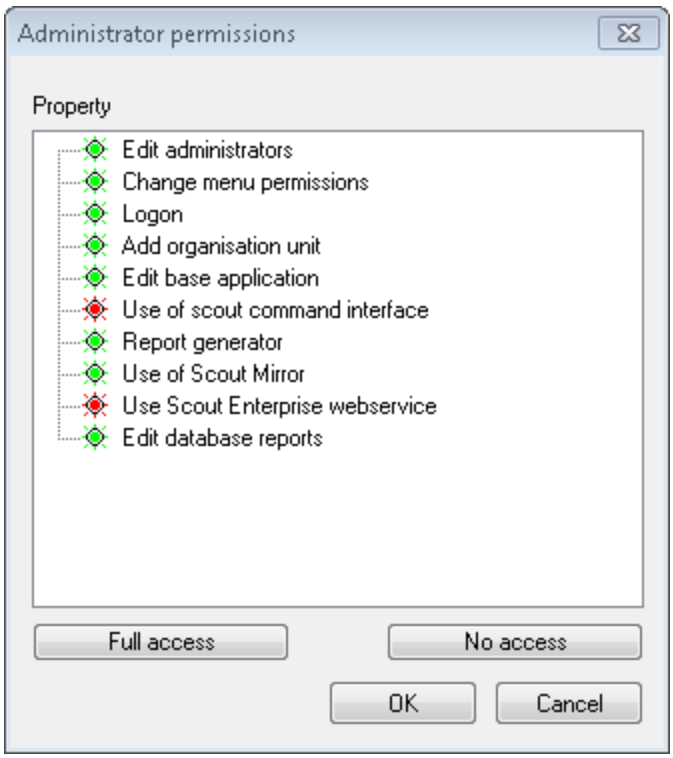
Important

For all kinds of permissions the following applies: If a permission is turned off, the relevant administrator has no longer access . For the last or the only administrator existing you cannot turn off access rights.This is to prevent being locked out of the Scout Enterprise console.

11.4.1. Changing base permissions

1. In Scout Enterprise console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Base permissions...**.

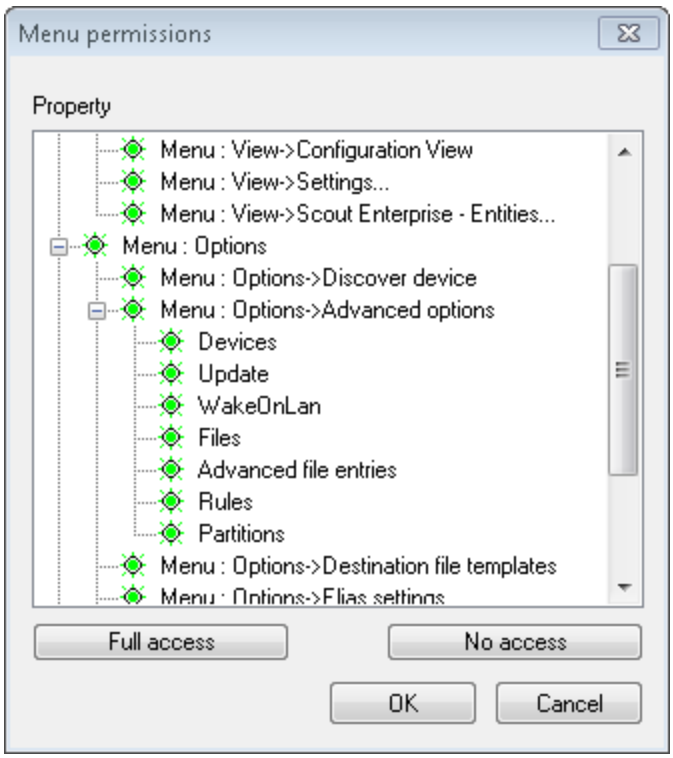
   *The **Administrator permissions > Base permissions** dialog opens.*
4. Change the relevant permissions by double-clicking or by using the SPACE bar.
5. Confirm with **OK**.



11.4.1. Changing menu permissions

1. In Scout Enterprise console, click **Security > Menu permissions...**.
2. In the **Menu permissions** dialog, select the relevant administrator.
3. Click **Menu permissions...**.

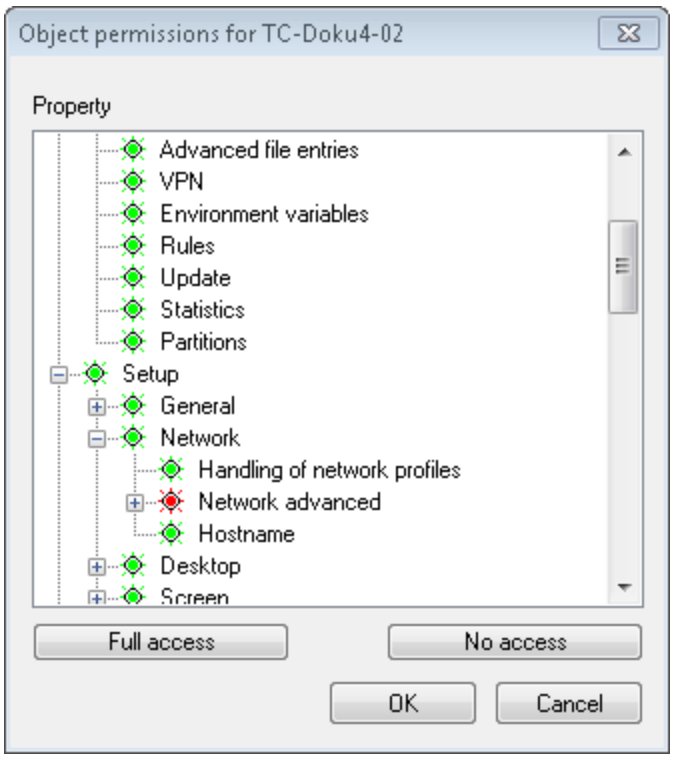
   *The **Menu permissions** dialog opens.*
4. Change the relevant permissions by doubleclicking or by pressing the SPACE bar.
5. Confirm with **OK**.



11.4.1. Changing object permissions

1. In Scout Enterprise console, select an OU or device.
1. Click **Security > Object permissions...**.
2. In the **Object permissions** dialog, select the relevant administrator.
3. Click **Object permissions...**.

   *The **Object permissions for ...** dialog opens.*
4. Change the relevant permissions by doubleclicking or by pressing the SPACE bar.
5. Confirm with **OK**.



11.4.1. Changing default object permissions

Default object permissions apply to all objects for which there are no specific rules defined .

1. In Scout Enterprise console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Default object permissions...**.

   *The **Default object permissions** dialog opens.*
4. Change the relevant permissions by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.

11.4.1. Defining a Start OU

This feature lets you deterrmine that an administrator is allowed to see only a particular start OU including its subordinate OUs.

1. In Scout Enterprise console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Set root OU ...**.

   *The **Root organisation unit** dialog opens.*
4. Check the **Use the following root organisation unit** option .
5. Select the relevant root OU.
6. Confirm with **OK**.

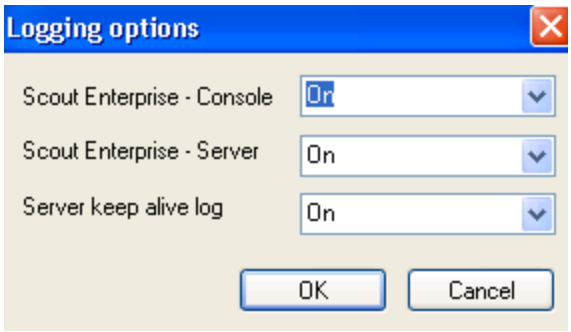
11.5. Passthrough Authentication

The Passthrough Authentication enables Single-Sign-On. Therefore, your Windows account information is used to automatically log you on to Scout Enterprise. The **Scout Enterprise log on** window won't be shown anymore.

11.6. Logging options

Using the Scout Enterprise Logging options you can define the features to be logged by enabling the relevant log files.

- In Scout Enterprise console, click **Options > Logging options** and enable or disable the relevant log files.



Logging option	Setting	Log file	Description
Scout Enterprise - Console	On	scout.log	The `scout.log` is created in your `Documents` directory under `\UniCon\Scout\Console` This file is only required for debugging. To open it in Scout Enterprise console click **View > System diagnostic > Console log**.

Logging option	Setting	Log file	Description
Scout Enterprise - Server	On	eluxd.log	`eluxd.log` is required for any support call. It is created in your `Public documents` directory under `\UniCon\Scout\Server` each time the Scout Enterprise Server starts. Previously generated files are renamed such as `eluxd.log.1, ..., eluxd.log.3`. To open a log file in Scout Enterprise console click **View > System diagnostic > Server log**.
Server keep alive log	On	KeepAlive.log	KeepAlive.log is created in your `Public documents` directory under `\Unicon\Scout\Server` and contains time stamps every 10 minutes. To open it in Scout Enterprise console click **View > System diagnostic > Server files**.

Note
Accessing the Scout Enterprise Server log requires Scout Enterprise console being installed in the same directory as Scout Enterprise Server.

12. Statistic Server

12.1. About statistic server

From Scout Enterprise version 13.5.0 the Scout Enterprise statistic server is included. Installation is possible via the InstallShield Wizard. The statistic server enables a evaluation of configurable status messages (keep alive messages) of the clients. Within a time interval defined the configured clients send a status message to the Scout Enterprise statistic server. Due to the transferred status messages the status will be modifyed correspondingly in the Scout Enterprise console.

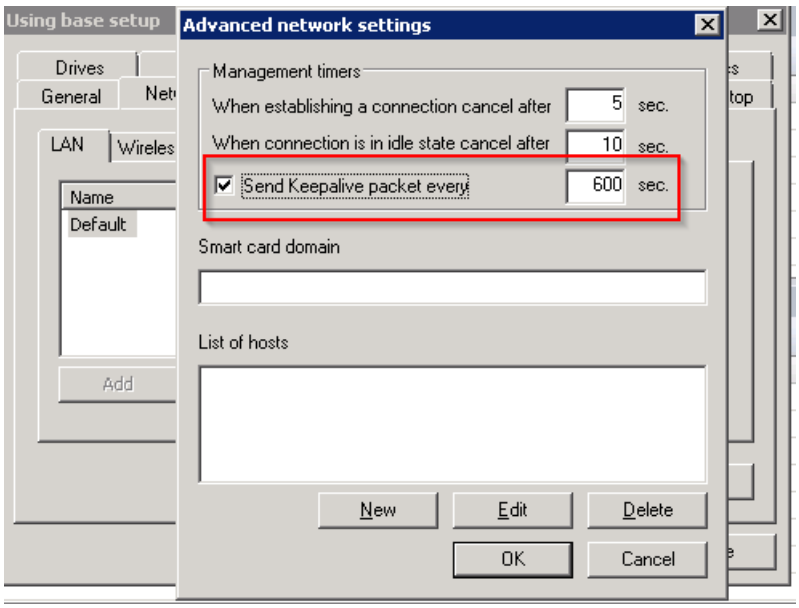
12.2. Requirements

To use the statistic server the following requirements are important:

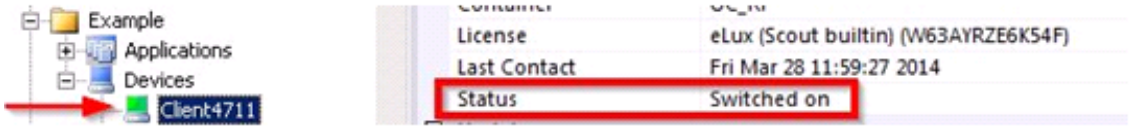
- Scout Enterprise version 13.5.0 or higher in use.
  Download the current Scout Enterprise version on www.myelux.com
- Valid Subscription
- eLux RP version 4.4.0 or higher

12.3. Defining status messages (keep alive message)

1. Start the Scout Enterprise console **> Options > Base configuration > Network > Advanced**
   Or: Right click on corresponding OU or device **> Configuration > Network > Advanced**.
2. Define the time interval in seconds.
   Within the time interval defined the configured clients will send the status message to the statistic server.



3. Due to the transferred status messages to the statistic server the status of the relevant devices or OU will be updated in the Scout Enterprise console.The clients are displayed with a green icon.



4. If the status message of a particular device is missing within the time interval defined, the device status in the Scout Enterprise console will be set to `Switched off` and the icon becomes red..

12.4. Examples of the status message

With the aid of the icons in the tree structure of the Scout Enterprise console you can identify the different messages:

-

  The client is properly working. Status messages are transferred successfully to the Scout Enterprise statistic server.

-

  The client underlies a time out from the network connection. Status messages can not be forwarded to the Scout Enterprise statistic server.

-

  The client is reconnected to the network connection. Status messages will be again forwarded to the Scout Enterprise statistic server.

13. Communication of the console

13.1. Closing the console

1. In Scout Enterprise console, click **File > Console Management > Close console**.

   *The **Close console** dialog opens.*

2. Click **Refresh** to receive an up-to-date list showing all active consoles.
3. Choose **Find** to filter the list.
4. If you want the user to receive a message, check the **Inform user for** option and enter the seconds as desired.
5. If you want to give the user the chance to cancel the command, check the **Command can be canceled by the user** option .
6. Select the relevant consoles in the list.
7. Click **Close selected consoles** or **Close all consoles**, respectively.

The command will be communicated to the consoles. Closing the consoles might take several minutes. The dialog waits up to 5 minutes for receiving the confirmation of all consoles. The list of all active consoles will be updated continuously within the time period.

13.2. Sending messages

With the aid of this function you can send messages to other console instances. Every console instance shows a message only once. If the console instances were not started within the whole period of validity the message will not be shown. If a user starts within the period of validity a console instance which was not yet involved in the database, the message will only be shown in the case the option **To all consoles** was activated.

1. Choose **Receiver**and which console should receive the message.
2. Choose in **time period** how long the message should be displayed.
3. Enter in **Message** the text.
4. The option **inform user...** closes the message located in the receiver console automatically after expiration of the time period stated.
5. The option **Command can be canceled by the user** enables the user to close the message in the receiver console without confirming the receipt of this particular message. In this case this particular message will be displayed again after a reboot of the console executed within the time of validity. If the time of validity is exposed and the user selected no button the message can be seen as received.
6. Choose **Send**.
   The message will be sent to the consoles selected.

13.3. Managing consoles

As soon as a console is opened by an administrator it is registered to the Scout Enterprise database. The registered consoles are displayed in the **Manage consoles** dialog.

- Click **File > Console management > manage consoles**.

For every console available, the signed-in user, the name of the computer as well as the sign in domain shown. The console activated is faded out in this case. If a user has various console instances opened on its computer, the consoles will be numbered serially. For example is "mfr #2" the second console instance of the user with the name "mfr". It is possible deactivating console instances by removing the tick in the corresponding dialog. This particular console instance will not any longer be displayed in the console communication in the other dialogs. Alternatively you can also delete the console instance. However, all commands concerning this particular console will also be deleted. In this case you will lose a part of the command history and possibly you will also lose commands which are not yet processed. This function is needed for deleting old, no longer used consoles from the memory. There is no affect of this procedure concerning currently opened and active consoles. You are able to check if all users are known in the Active Directory. Unknown users can be selected and can possibly be deleted or added to the Active Directory. The button Search fades in for every column in the list. The place holders '*' and '?' are accepted within the search text, the use of capital and small initial letters will be ignored. By clicking the button **X** the search field will be closed.

13.4. Managing commands

Any console commands that have been run such as **Close console...** and **Send message...** can be viewed. Moreover, in the bottom list, the receiving consoles can be viewed and filtered.

Displaying commands

1. If you want to filter the commands, use one of the the options: **All**, **Active**, **Inactive**, **Older than** and **Younger than**.
2. If you want to display a search field for one of the columns, click **Find**.

Changing validity of commands

- Select a command and modify date and time under **Valid until**.

Deleting commands

1. If you want to delete all commands, click **Delete all**.
2. If you want to delete a particular command, select the command and click **Delete**.

14. Import/Export

14.1. General

All functions can either be applied via Scout Enterprise Console or SCMD-Interface. Further information to SCMD can be found at the SCMD documentation.

The export files will be saved in XML format. The filename extension depends on the data category.

Data category for export/import	Filename extension
Configuration of OUs	.oustp
Configuration of devices	.devstp
Properties of OUs	.oupro
Properties of devices	.devpro
Properties of applications	.apppro
Device list	.csv
OU tree	.outree

These files can be edited using Scout Enterprise Configuration Editor. You can start this program using **Start > Programs > Scout Enterprise > Configuration Editor**.

14.2. Exporting

1. Select the OU you want to export data from.
2. Click **File > Export** and what you want to export.
3. Select a folder to save and apply with **OK**.

14.3. Importing

1. Select the OU you want to import data into.
2. Click **File > Import** and the data category you want to import.
3. Apply with **OK**.

15. Optimizing and troubleshooting

15.1. Optimizing with handshake

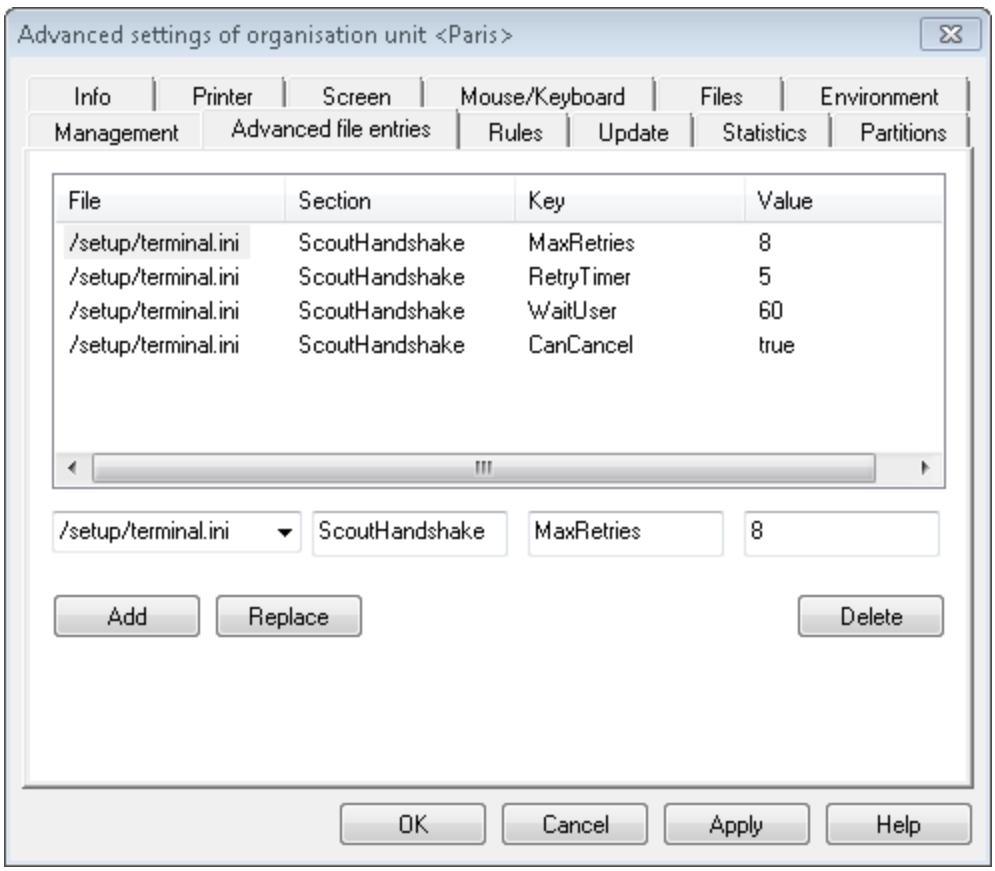
During each start-up the thin clients contact their Scout Enterprise server and check for new configuration data and application definition data. If they don't reach the Scout Enterprise server, they retry to connect and synchronize according to their handshake configuration.

Activating new configuration data might require a restart of the client. Then the user is informed and has the chance to suppress restarting

.

Handshake parameters can be set in the `terminal.ini` file of the client using the **Advanced file entries** feature. For more information, see Advanced file entries.

Handshake can be configured for the entire organization or for a particular OU or device.



The values shown in the figure above are examples and can be modified.

The section `ScoutHandshake` provides four configurable parameters:

Parameter	Description
MaxRetries	Number of connection attempts The value `0` deactivates handshake.

Parameter	Description
RetryTimer	Period of time in seconds until next connection attempt (start value) After each attempt the interval is doubled (+/- random value). Example: Having defined `8` connection retries and a **RetryTimer** start value of `5` seconds, the 8. connection attempt is carried out after 22 minutes.
WaitUser	Waiting time before client restarts to give the user the chance to close applications or log off.
CanCancel	Defines, if the user is allowed to suppress restart of the client device (`true` | `false`).

15.2. Error messages during Scout Enterprise setup

If you use the **eLux AllPackages** download package, the following error messages might appear during installation:

File can't be created in the indicated directory

Solution: Provide a different directory.

File access error while checking HTTP/FTP server (error number = 404)

This message is possibly caused by missing MIME type entries for the file extensions `.idf`, `.epm`, `.fpm` and `.gz` as text/plain.

Solution: Add the Scout Enterprise Mime types to Microsoft Internet Information Server (IIS) by executing the VB script `ScoutAddMimeTollS.vbs`:

1. Download from www.myelux.com **eLux Software Packages > eLux RP Container > Released packages >** *Latest version* **> Bundles > eLuxRP-*_AllPackages** the file `AllPackages.zip`. Follow the next instructions in order to execute the VBS script ScoutAddMimeTollS.vbs which will add the Scout Enterprise MIME type to the. The VBS script must be run with administrator privileges.
2. Open the `zip` file and the subfolder `Support`. Copy the file `ScoutAddMimeTollS.vbs` to `C:\temp`.
3. Execute the VBS script with admin rights.

   *The message **Add Scout MIME types to Internet Information Server** is shown.*
4. Confirm with **OK**.

   *The message **Added MIME types successfully** is shown.*

Note
Where required, the VB script must be run in the Windows command shell in C:\TEMP using the command `wscript ScoutAddMimeToIIS.vbs`.

16. Appendix

16.1. Port assignments

Below you find a list of TCP/IP ports for eLux and Scout Enterprise. The port numbers are fixed. Exceptions are indicated with a footnote.

eLux

Port	Type	Specification	How to deactivate	Port Type
	ESP	VPN (Cisco)	Uninstall the package Cisco Systems VPN client (cisco_vpnclient)	Incoming
	ESP	VPN (Cisco)	Uninstall the package Cisco Systems VPN Client" (cisco_vpnclient)	Outgoing
21	TCP	Update via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	3270, 5250, 97801 emulations and telnet sessions		Outgoing
37	TCP	Time Server – RFC 868	Do not configure a time server (**Setup > Desktop**)	Outgoing
37	UDP	Time Server – RFC 868	Do not configure a time server (**Setup > Desktop**)	Outgoing
53	TCP	DNS server (Windows)		Outgoing
53	UDP	DNS server		Outgoing
67	UDP	DHCP server	Configure a local IP address (**Setup > Network**)	Outgoing
68	UDP	DHCP client (or: BootP client)	Configure a local IP address (**Setup > Network**)	Incoming
69	UDP	TFTP server (only used during a recovery installation)		Outgoing
69	UDP	TFTP server (only used during a recovery installation)		Incoming
80	TCP	Updating by using HTTP (and proxy port, if used)		Outgoing

Port	Type	Specification	How to deactivate	Port Type
102	TCP	Emulations for BS2000 mainframes		Outgoing
111	UDP	Port mapper – drive access on NFS servers. Works with NFSD drive access (port 2049) and mountd (random)	Uninstall the FPM drive support (automount) in baseOS	Outgoing
111	TCP	Port mapper – RPC internal use only. Wokrs with nlockd (random)	Uninstall the FPM drive support (automount) in baseOS	Incoming
139	TCP	SMB drive mapping (NetBIOS) and SMB user authentication	Uninstall the FPM drive support (automount) in baseOS and the package User authorisation modules (userauth)	Outgoing
139	UDP	SMB drive mapping (NetBIOS) and SMB user authentication	Uninstall the FPM drive support (automount) in baseOS and the package User authorisation modules (userauth)	Outgoing
161	UDP	SNMP	Uninstall the package net-snmp (snmp)	Incoming
161	UDP	SNMP	Uninstall the package net-snmp (snmp)	Outgoing
162	UDP	SNMPTRAP	Uninstall the package net-snmp (snmp)	Outgoing
177	UDP	XCMCP protocoll		Outgoing
389	TCP	LDAP user authentication		Outgoing
500	UDP	VPN (Cisco)	Uninstall the package Cisco systems VPN client (cisco_vpnclient)	Incoming
500	UDP	VPN (Cisco)	Uninstall the package Cisco systems VPN client (cisco_vpnclient)	Outgoing
514	TCP	Shell, X11 applications		Outgoing
515	TCP	Printing via LPD	Uninstall the package print environment (CUPS) (baseprinter)	Outgoing
515	TCP	Printing via LPD	Uninstall the package print environment (CUPS) (baseprinter)	Incoming
631	TCP	CUPS (IPP) print client	Uninstall the package “Print Environment (CUPS)" (baseprinter)	Outgoing

Port	Type	Specification	How to deactivate	Port Type
631	UDP	CUPS (IPP) Druckclient	Uninstall the package "Print Environment (CUPS)" (baseprinter)	Outgoing
2049	UDP	NFSD drive access NFS	Uninstall the FPM drive support (automount) in baseOS	Outgoing
5681	TCP	Scout Enterprise Management port		Incoming
5900	TCP	Mirroring eLux desktop	Disable mirroring (**Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Incoming
5901	TCP	Mirroring first XDMCP session	Disable mirroring (**Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Incoming
5902	TCP	Mirroring second XDMCP session	Disable mirroring (**Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Incoming
6000	TCP	Remote X11 application	Clear checkbox **Setup > Security > Allow remote X11 clients**	Incoming
6001	TCP	first XDMCP session		Incoming
6002	TCP	second XDMCP session		Incoming
7100	TCP	Font server[1]		Outgoing
20000	UDP	Wake-on-Lan		Incoming
20000	UDP	Wake-on-Lan		Outgoing
22123	TCP	Scout Enterprise Manager (secure)		Incoming
22123	TCP	Scout Enterprise Manager (secure)		Outgoing
7777	TCP	Scout Enterprise Manager		Incoming
7777	TCP	Scout Enterprise Manager		Outgoing
9100	TCP	Direct print to parallel port[2]	Clear checkbox **Setup > Printer > TCP direct print**	Incoming
9101	TCP	Direct print to USB port[3]	Clear checkbox **Setup > Printer > TCP direct print**	Outgoing

[1]The port number can be assigned by the administrator in the eLux control panel (**Setup > Screen > Advanced)**.
[2]The port number can be assigned by the administrator in the eLux control panel**Setup > Printer**).
[3]The port number can be assigned by the administrator in the eLux control panel**Setup > Printer**).

Scout Enterprise Server

Port	Type	Specification	How to deactivate	Port type
7779	TCP	Wake-On-LAN gateway		Outgoing
22123	TCP	Scout Enterprise Manager (secure)		Incoming
22123	TCP	Scout Enterprise Manager (secure)		Outgoing

Scout Enterprise Console

Port	Type	Specification	How to deactivate	Port type
5900	TCP	Mirroring the eLux desktop	Deactivate mirroring via the checkbox (**Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Outgoing
5901	TCP	Mirroring of the first XDMCP session	Clear mirroring via the checkbox **Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Outgoing
5902	TCP	Mirroring of the second XDMCP session	Deactivate mirroring via the checkbox (**Setup > Security**) or uninstall the package mirror eLux desktop (mirror)	Outgoing

16.2. SNMP

SNMP (Simple Network Management Protocol) is a network protocol which enables the query of status information and provides the definition of configuration parameters.

The software package snmp-5.6.1.1-2 must be installed for the configuration of SNMP .

1. Download at **www.myelux.com > eLux Software Packages > eLux RP Container > Released Packages > Add-On > snmp-5.6.1.1-2**.

   Note

   The command line program snmpget is not integrated in the software package. For the query of SNMP status information, please use a software provided by a third party supplier.

2. Choose from two methods in order to setup SNMP:
   A) Transfer the configuration file snmpd.conf to /setup/snmpd.conf.

   Or:

   B) Use Advanced file entries in Scout Enterprise.
   Example:
   File: /setup/terminal.ini
   Section: SNMPD
   Entry: rocommunity
   Value: secret

   Note

   If the file /setup/snmpd.conf is present then this configuration method has priority.
   If this file is not present the section [snmpd] will be evaluated in the terminal.ini.
   If the section [snmpd] is also not available, the read only community "public" will be created.
   Then you can test by using the local shell (XTERM) as follows:
   snmpget -v 2c -c public <ip-address> SNMPv2-MIB::sysName.

3. In the section [SNMPD], you can enter more of the so called SNMPD Configuration Directives, for example "syscontact" or "syslocation" in order to modify the configuration.
   The Configuration Directives control:
   - the access rights to the SNMP agent.
   - the information that is supplied by the SNMP agent.
   - the active monitoring of the local system.
   - the extension of the SNMP agent's functionality.

4. For debugging purposes you can enter further commands in the section [SNMP]. These commands are the so called "SNMP Configuration Directives". Again using the advanced file entries, you can e.g. set the entry "doDebugging" to the value "1" in the section [SNMP] of the file "terminal.ini".

16.3. SNMPD and SNMP Configuration Directives

The following table refers to the software package snmp-5.6.1.1-2 in combination with eLux. Further information regarding the use of SNMP can be found here. Detailed information regarding SNMP commands can be found here.

SNMPD Configuration Directives

Application	Command
authtrapenable	1 | 2 (1 = enable, 2 = disable)
trapsink	host [community] [port]
trap2sink	host [community] [port]
informsink	host [community] [port]
trapsess	[snmpcmdargs] host
trapcommunity	community-string
agentuser	agentuser
agentgroup	groupid
agentaddress	SNMP bind address
syslocation	location
syscontact	contact-name
sysservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1|v2c|usm security
access	name context model level prefx read write notify
view	name type subtree [mask]
rwcommunity	community [default|host-name|network/bits] [oid]
rocommunity	community [default|host-name|network/bits] [oid]
rwuser	user [noauth|auth|priv] [oid]
rouser	user [noauth|auth|priv] [oid]
swap	min-avail
proc	process-name [max-num] [min-num]

Application	Command
procfix	process-name program [arguments...]
pass	miboid command
pass_persist	miboid program
disk	path [minspace | minpercent%]
load	max1 [max5] [max15]
exec	[miboid] name program arguments
sh	[miboid] name program-or-script arguments
execfix	exec-or-sh-name program [arguments...]
file	file [maxsize]
dlmod	module-name module-path
proxy	[snmpcmd args] host oid [remoteoid]
createUser	username (MD5|SHA) passphrase [DES] [passphrase]
master	pecify 'agentx' for AgentX support
engineID	string
engineIDType	num
engineIDNic	string

SNMP Configuration Directives

Application	Command
doDebugging	(1|0)
debugTokens	token[,token...]
logTimestamp	(1|yes|true|0|no|false)
mibdirs	[mib-dirs|+mib-dirs]
mibs	[mib-tokens|+mib-tokens]
mibfile	mibfile-to-read
showMibErrors	(1|yes|true|0|no|false)
strictCommentTerm	(1|yes|true|0|no|false)
mibAllowUnderline	(1|yes|true|0|no|false)
mibWarningLevel	integerValue

Application	Command
mibReplaceWithLatest	(1|yes|true|0|no|false)
printNumericEnums	1|yes|true|0|no|false)
printNumericOids	1|yes|true|0|no|false)
escapeQuotes	(1|yes|true|0|no|false)
dontBreakdownOids	(1|yes|true|0|no|false)
quickPrinting	(1|yes|true|0|no|false)
numericTimeticks	(1|yes|true|0|no|false)
suffixPrinting	integerValue
extendedIndex	(1|yes|true|0|no|false)
printHexText	(1|yes|true|0|no|false)
dumpPacket	(1|yes|true|0|no|false)
reverseEncodeBER	(1|yes|true|0|no|false)
defaultPort	integerValue
defCommunity	string
noTokenWarnings	(1|yes|true|0|no|false)
noRangeCheck	(1|yes|true|0|no|false)
defSecurityName	string
defContext	string
defPassphrase	string
defAuthPassphrase	string
defPrivPassphrase	string
defVersion	1|2c|3
defAuthType	MD5|SHA
defPrivType	DES (currently the only possible value)
defSecurityLevel	noAuthNoPriv|authNoPriv|authPriv